SierraNet M408

User Manual

Software Version 1.70

Generated: December 15, 2014, 09:58

Teledyne LeCroy Protocol Solutions Group

Trademarks and Servicemarks

Teledyne LeCroy, CATC Trace, and SierraNet Protocol Suite are trademarks of Teledyne LeCroy.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Intel and Pentium are registered trademarks of Intel Corporation.

All other trademarks and registered trademarks are property of their respective owners.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL INFORMATION, EXAMPLES AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE REPRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS ARE FULLY RESPONSIBLE FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN INFORMATION THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT Teledyne LeCroy FOR A COPY.

WEEE Program

This electronic product is subject to disposal and recycling regulations that vary by country and region. Many countries prohibit the disposal of waste electronic equipment in standard waste receptacles. For more information about proper disposal and recycling of your Teledyne LeCroy product, please visit teledynelecroy.com/recycle.

Teledyne LeCroy
3385 Scott Blvd.
Santa Clara, CA 95054
TEL: 800-909-7112 (USA and Canada)
TEL: 408-653-1260 (worldwide)

Contents

Chapter 1

Introduction

This manual describes installation and operation of the Teledyne LeCroy SierraNet M408™ Fibre Channel over Ethernet (FCoE) Protocol Analyzer and includes examples of typical applications.

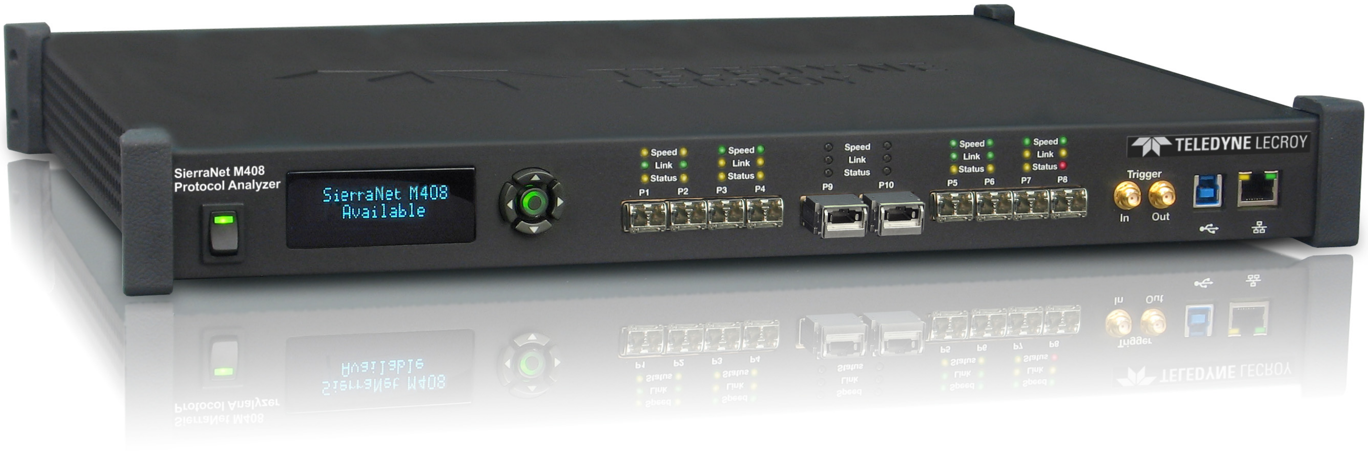


Figure 1.1 Teledyne LeCroy SierraNet M408 Protocol Analyzer

1.1 Analyzer Overview

The SierraNet M408 analyzer is Teledyne LeCroy's 10 Gigabit Ethernet, 40 Gigabit Ethernet and 16 Gigabit Fibre Channel Analyzer and Jammer platform. The M408 has eight SFP+ 10GigE / 16G FC and two QSFP 40GigE ports. The M408 is very portable and can also be rack mounted (1U form-factor). Up to 64 GB of capture memory allow extensive line-speed capturing. The analyzer supports “Super Jumbo” packets up to 64K.

The M408 ports allow signals to pass through without re-timing, ensuring that the test platform is as transparent as possible.

The analyzer can be controlled either via an 1GbE connection to the local network or via a USB connection. The SierraNet M408 provides the user with an easy to understand control panel and LED indicators.

Major features of the M408 include triggering on back-to-back events, use of counters within trigger conditions, and multi-state (up to 24) triggering and filtering state machines with four transitions per state.

1.1.1 Receiving Your Analyzer

The analyzer package includes the following components:

- ❑ SierraNet M408 Analyzer identified in the packing list
- ❑ SierraNet M408 Quick Start
- ❑ USB A-B 3.0 cable, 1 meter
- ❑ USB A-B 2.0 cable, 1.8 meter
- ❑ Ethernet cable, 10 feet
- ❑ Three-Prong AC power cord
- ❑ C13-C14 10A power cord, 2 meter
- ❑ Installation CD ROM with software and documentation

1.1.2 Unpacking the Analyzer

Inspect the received shipping container for any damage. Unpack the container and account for each of the system components listed on the accompanying packing list. Visually inspect each component for absence of damage. In the event of damage, notify the shipper and Teledyne LeCroy. Retain all shipping materials for shipper's inspection.

1.1.3 Analyzer Features

The Analyzer has the following features:

- ❑ Power Switch
- ❑ Speed, Link and Status LEDs (see next page)
- ❑ Ports 1 and 2 connector pair
- ❑ Ports 3 and 4 connector pair
- ❑ Ports 5 and 6 connector pair
- ❑ Ports 7 and 8 connector pair
- ❑ Ports 9 and 10 connector pair
- ❑ Status and Configuration LCD Display
- ❑ Front Panel Configuration Buttons
- ❑ External Trigger Input and Output
- ❑ USB port for host connectivity
- ❑ Ethernet port for network connectivity
- ❑ CrossSync Control Panel

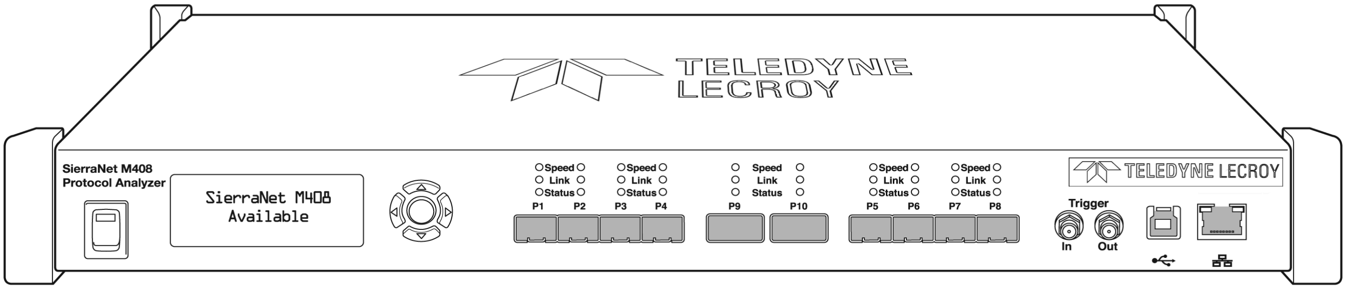


Figure 1.2: Front Panel

On the back, the Analyzer has:

- ❑ Power In

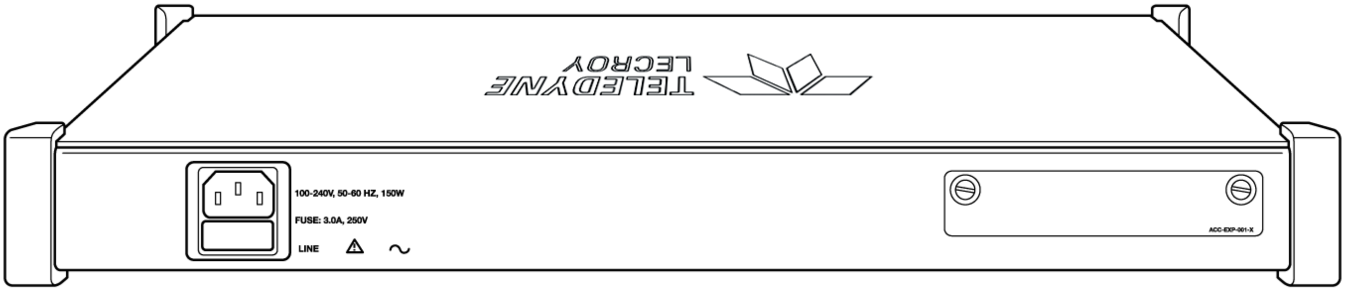


Figure 1.3: Back Panel

1.1.4 LEDs

LEDs indicators support each port link pair (P1 - P2; P3 - P4; P5 - P6; P7 - P8 and P9 -10) with the following functionality (see Figure 1.4):

Speed LEDs

The LEDs for SPEED illuminate as follows:

	GBE	**Fibre Channel**
Yellow	🟡 Reserved	🟡 4G/2G/1G FC
Green	🟢 10 GigE	🟢 8G FC
Blue	🔵 40 GigE	🔵 16G FC

Link Activity LEDs

Green	🟢 Network activity Detected
Yellow	🟡 Link up, no activity
No Color	⚪ No link

Status LEDs

Yellow Blinking	◒ Waiting for trigger
Yellow Solid	🟡 Triggered
Red	🔴 Error detected
No Color	⚪ No Activity

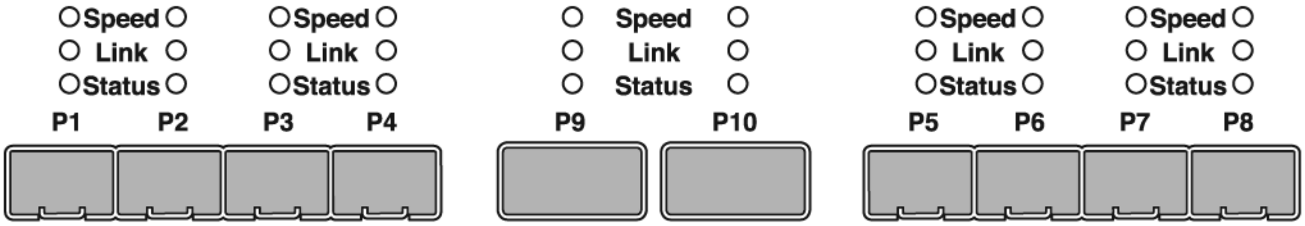


Figure 1.4: LEDs on the Front Panel

1.1.5 Status and Configuration Display

The Analyzer front LCD display indicates the configuration and status of the device. For example, during initialization, the LCD panel displays boot status messages.

1.1.6 LCD Display and Button Functions for Configuring the Analyzer

The basic settings of the SierraNet M408 can be configured from the unit itself. Five buttons are provided to enable you to configure the Analyzer. When you first turn on the Analyzer, after initialization, the LCD displays **SierraNet M408 Available** with two arrows pointing up and down as shown in the illustration below.

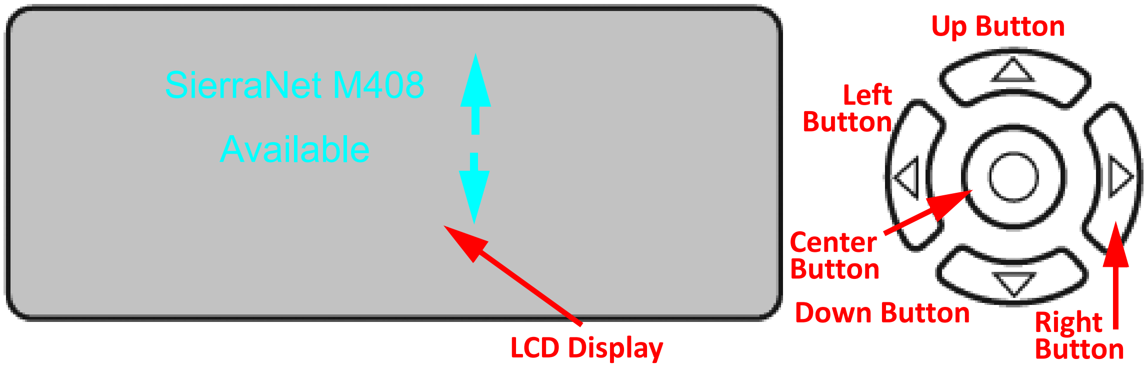


Figure 1.5: LCD Display and Button on the Front Panel

When connected via ethernet or USB, the **Up** ⇑ and **Down** ⇓ buttons display the following:

- ❑ Displays current Static or Dynamic IP Address
- ❑ SierraNet M408 SN (serial number)
- ❑ Connection
- ❑ Unit Name
- ❑ Set IP Configuration
- ❑ IP Mode Dynamic, or
- ❑ IP Mode Static

The **Left** ⇐ and **Right** ⇒ buttons are used to change the configuration properties.

The LCD will display **Button Inactive In This MenuItem** if the button does not serve any purpose for that selection.

Perform the following steps to set IP Configuration, Static on Dynamic IP using the buttons and the LCD display on the Analyzer:

Set IP Configuration

To set IP Configuration:

1. Press the **Up Button** once to get into the **Set IP Configuration** mode.
2. Press the **Center Button** once to select Set IP Configuration**.**

Set IP Mode Static is displayed in the LCD display. If you do not want to set IP Mode Static, press the **Up Button** to set the IP Mode Dynamic, see "IPMode Dynamic" on page 6).

3. Press the **Center Button** once to select Set IP Mode Static**.**

   The **Static IP** address (for example: 188.168.040.036) is displayed in the LCD display.

4. Press the **Center Button** once to set the Static IP address**.**

   The first numeral of the IP address will start blinking.

5. Use the **Up Button** or **Down Button** to change the IP Address.
6. Press the **Right Button** or **Left Button** to move to the right or left to change each component of the static or dynamic IP address and change it using step 5.
7. Once the IP Address is set, press the center button to select it.
8. Press the **Up Button** once to **Accept and Reboot**.
9. Press the **Up Button** once to **Cancel** the Changes.
10. Press the **Up Button** once to set the **Gateway** address. Repeat steps 4 through 9 to set the Gateway address.
11. Press the **Up Button** once to set the **Subnet Mask** address. Repeat steps 4 through 9 to set the Subnet Mask address.
12. Press the **Up Button** once to set the **Static IP** address. Repeat steps 4 through 9 to set the Static IP address.
13. Press the **Center Button** once to confirm reboot. The LCD display will read **Center Button to Confirm Reboot.**
14. The Analyzer will reboot. The LCD display will display the new IP Configuration.

IPMode Dynamic

Perform the following steps to set IP Mode Dynamic on the Analyzer:

1. Press the **Up Button** once to get into the **Set IP Configuration** mode.
2. Press the **Center Button** once to select Set IP Configuration**.**

   Set IP Mode Dynamic is displayed in the LCD display.

3. Press the **Center Button** once to select Set IP Mode Dynamic**.**

   The **Dynamic IP** address (for example: 188.168.040.036) is displayed in the LCD display.

4. Press the **Center Button** to select it.
5. Press the **Up Button** once to **Accept and Reboot**.
6. Press the **Up Button** once to **Cancel the Changes**.

Note: In case the device is often moved from one subnet to the other, it is recommended to configure the DHCP server so that the device always receives the same (known) IP address. Many DHCP server allow this type of static allocation based on the devices MAC address.

1.2 Installing Your Analyzer

1.2.1 Software Installation

The software works on systems using the Windows® XP, Windows Server 2003, Windows Server 2008 R2, Windows Server 2012, Windows 7 and Windows 8/8.1 operating systems.

1. Insert the Installation CD-ROM into the CD drive on the host machine.
2. The installation automatically starts setup, unless Auto Run is off. In that case, select the CD-ROM from “My Computer” and click **Setup**.
3. After the warning to close all other programs and before starting the installation, the Install component selection opens.
4. Select components for installation.
5. Click **Next** to complete the installation.

System restart

You must restart your computer before you can use your Analyzer software.

Error Message

If you get an error message during installation of the drivers for Windows, consult your system administrator. Your system may allow only administrator-level users to copy such driver files.

1.3 Hardware Setup

The hardware setup is described below.

1.3.1 Connecting in General

Note: You must install the software before connecting the analyzer to the host machine for the first time.

To set up the analyzer:

1. Connect the analyzer to a 100V–240V, 50Hz–60Hz, power outlet and turn on the Power switch.
   At power on, the analyzer will go through initialization as shown on the LCD display.
2. Connect the USB cable between the SierraNet M408 USB port and a USB port on the Host PC. The host PC operating system detects the analyzer and configures the drivers automatically.
   (See “Connecting via Ethernet” on page 21 for Ethernet connectivity.)
3. Connect the analyzer as shown in the following figure. The following figure shows connections between Port-pairs P1-P2 to Device 1 and Device 2; P3-P4 to Device 3 and Device 4; and so on.

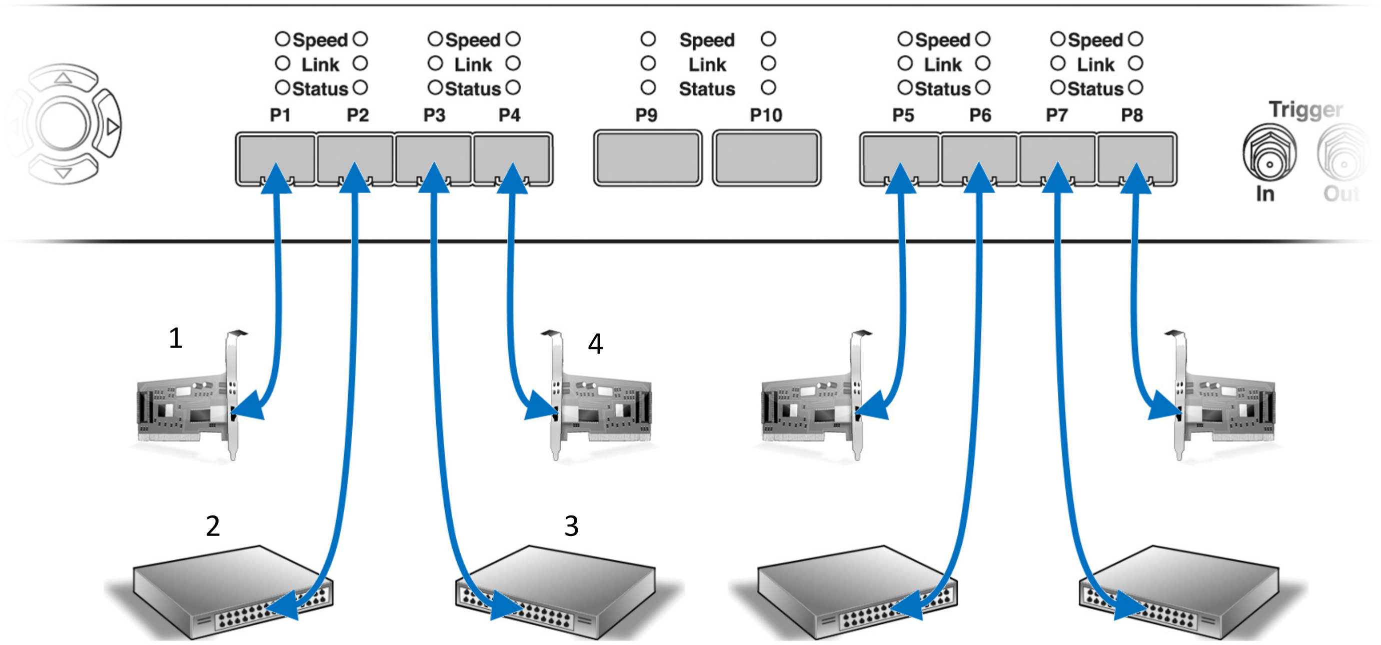


Figure 1.6: Analyzer Connections

1.3.2 Cables to Use

Connect to and from devices using SFP+/QSFP and a cable suitable for your setup.

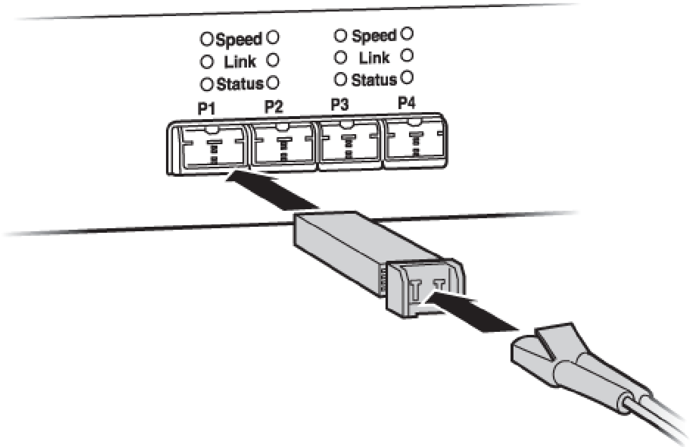


Figure 1.7: Analyzer Connections

1.4 Expandability

You can expand the functionality of the tester by daisy-chaining multiple SierraNet M408 analyzers with CATC SYNC Expansion Cards (ACC-EXP-002-X).

You can remove expansion cards with two simple tools.

1.4.1 Removing Expansion Cards

You can remove expansion cards using two tools:

- ❑ Standard (flat blade) 3/16” screwdriver
- ❑ Teledyne LeCroy Extraction Tool (part number 230-0160-00)

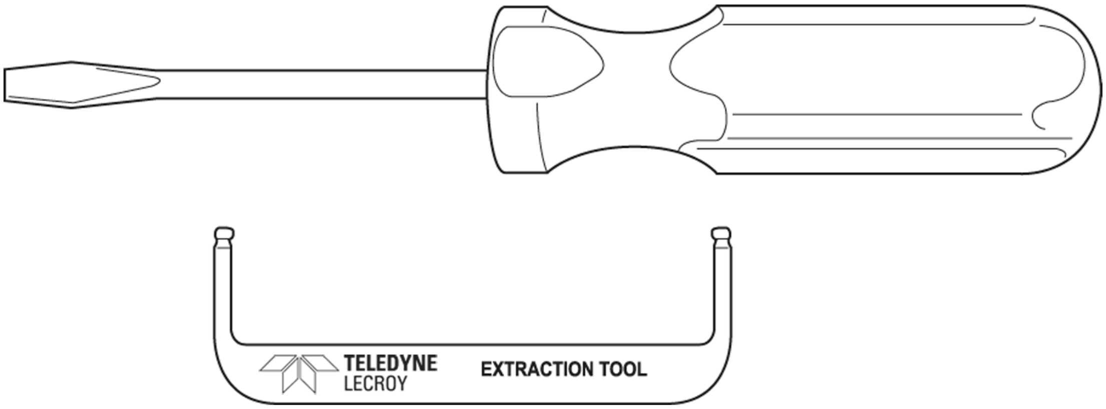


Figure 1.8: Tools needed to Remove the Expansion Cards

Note: The SierraNet M408 Protocol Analyzer does not support the power expansion card shown below. However, the method of inserting and removing any expansion card is the same.

To remove an expansion card, follow these steps:

1. Unplug the system from AC power and turn the system so the expansion port is facing you. Note the two retaining screws and the holes for the extraction tool that are located on the panel of the expansion card.

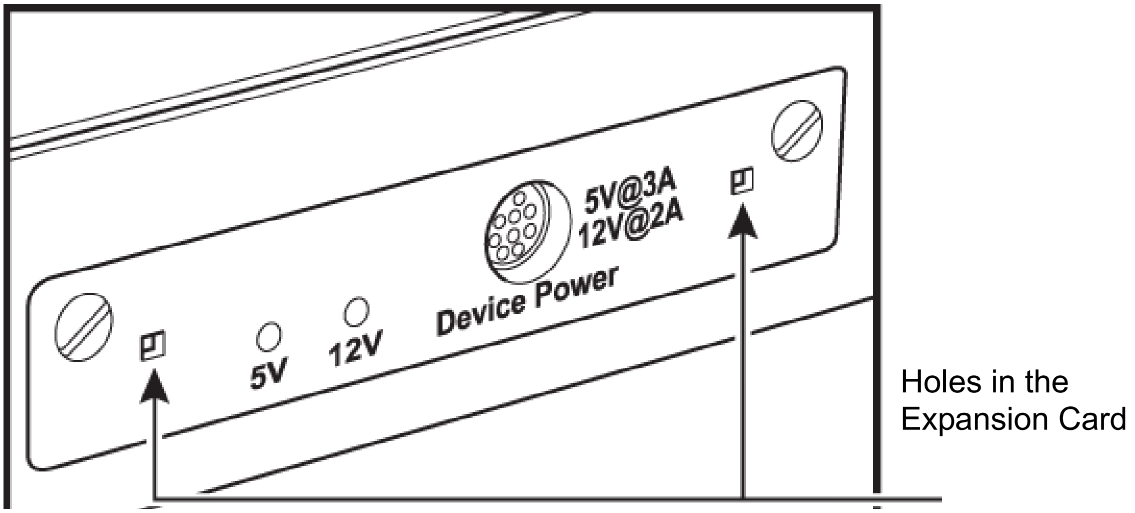


Figure 1.9: Holes in the Expansion Card Panel

2. Insert the extraction-tool prongs into the holes in the expansion card panel.

Note: If the prongs do not slip easily into the holes, use a small nail file or similar device to remove paint from the prongs

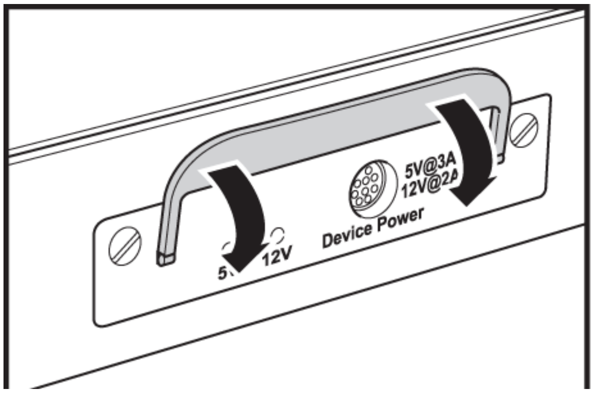


Figure 1.10: Insertion of Handle/Tool into Expansion Card Panel

3. Rotate the extraction tool to a horizontal position to lock the prongs into place and make a handle

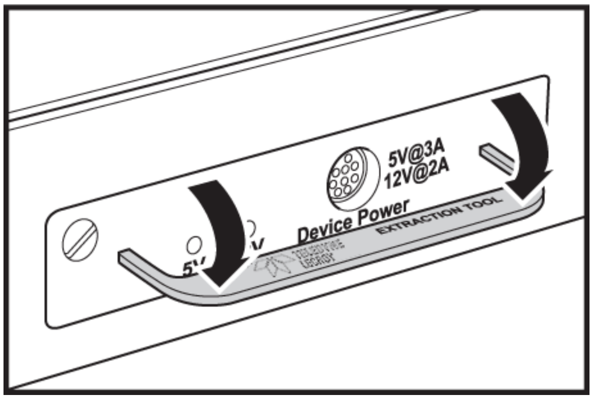


Figure 1.11: Rotate Handle/Tool from Vertical to Horizontal

4. Using the screwdriver, loosen both retaining screws by rotating them counter-clockwise approximately two full turns, until feeling slight resistance. **Do not force the retaining screws** after two turns.

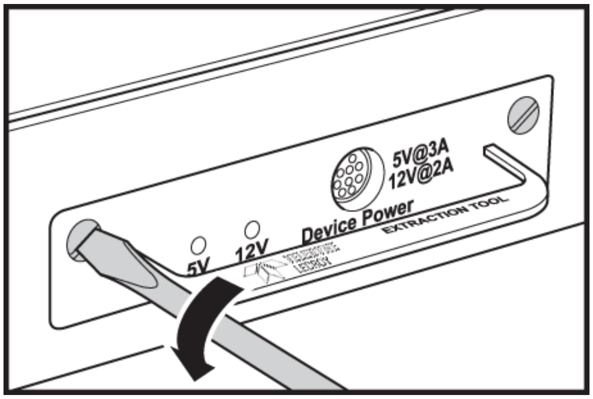


Figure 1.12: Loosen Screws with Flat Bladed Screw Driver

5. Using the extraction tool as a handle, gently wriggle the expansion card forward about 1/8".

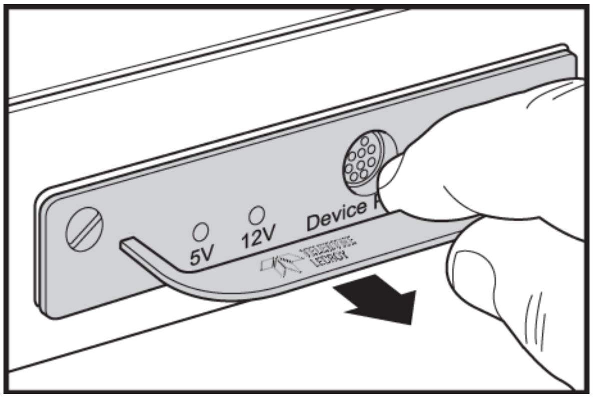


Figure 1.13: Pulling on the Expansion Card

6. Repeat steps 4 and 5 approximately three times, until the card is free from the retaining screws and you can remove the card from the system.

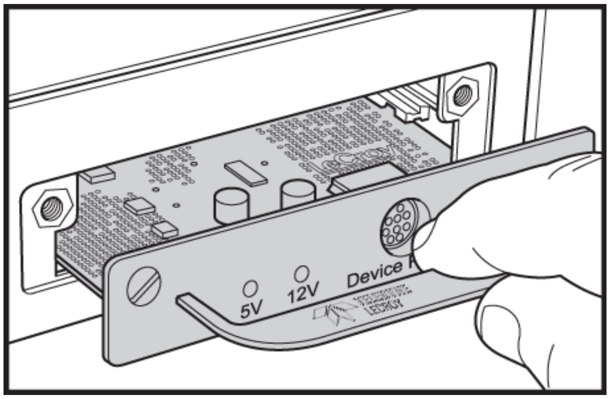


Figure 1.14: Remove Expansion Card from Chassis

1.4.2 Daisy-Chaining with CATC SYNC Expansion Cards

You can daisy-chain analyzer units for higher port count, by connecting the units through the optional CATC SYNC Expansion Card on the analyzer back.

Connecting Two SierraNet M408 Analyzers via the CATC Sync Expansion Card (ACC-EXP-002-X)

Multiple SierraNet M408 Analyzers can be connected using their CATC Sync ports which require an optional expansion card (ACC-EXP-002-X).

Note: Refer to relevant protocol analyzer user manual for instructions on how to install the expansion card.

To do so perform the following steps:

1. Make sure to stop any recordings in progress.

Note: You may plug/unplug the sync cable while the analyzer unit is powered on.

2. Connect the female end of the sync cable to the SYNC OUT port of one SierraNet M408.
3. Connect the male end of the sync cable to the SYNC IN port of the other SierraNet M408 (see Figure 1.15 on page 12.)

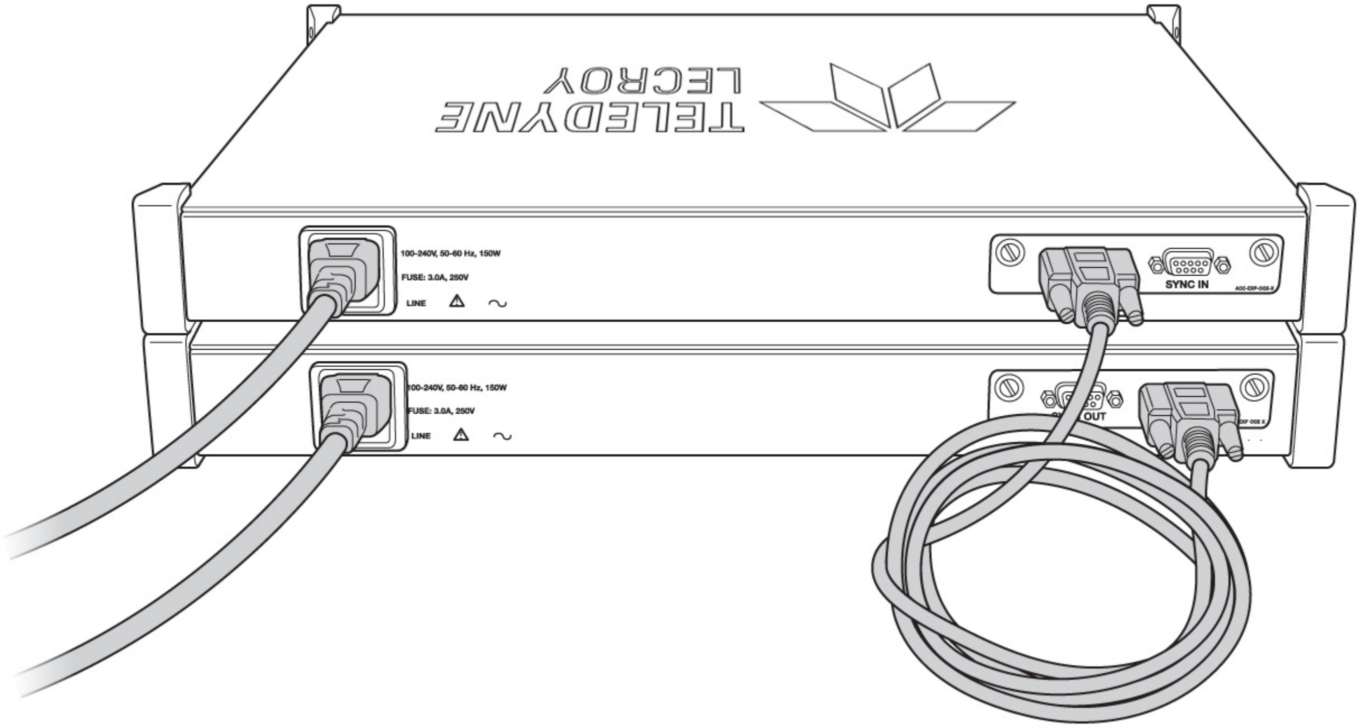


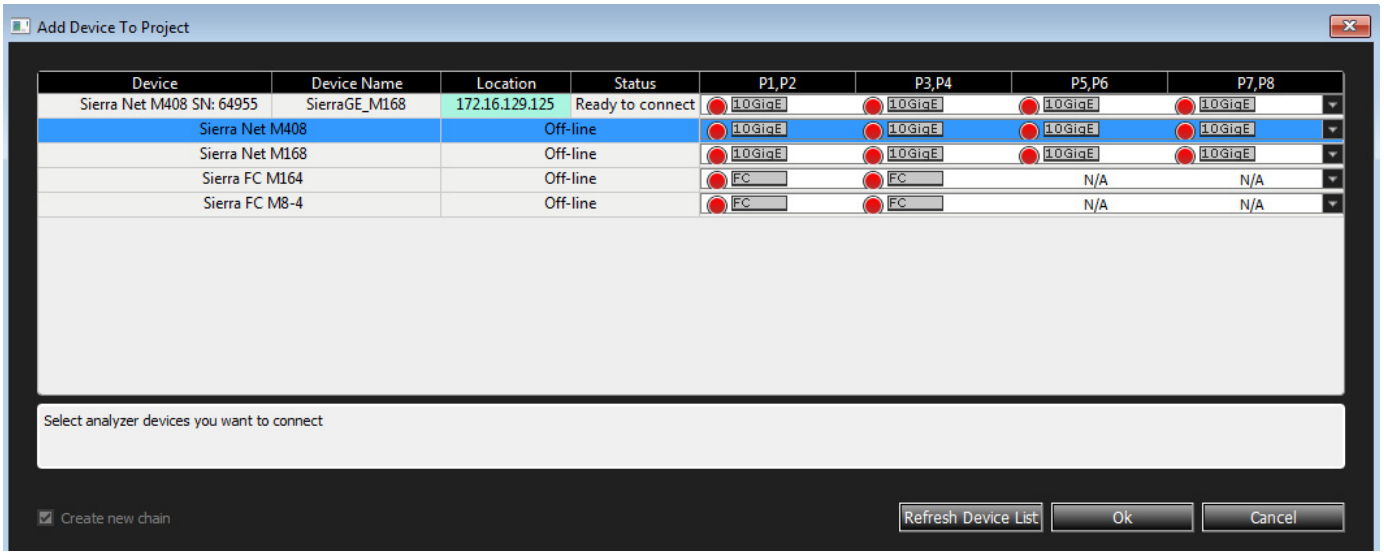
Figure 1.15: An Example of Connecting two SierraNet M408 Analyzers

Connecting to Sierra FC M8-4 and Sierra FC M164 Analyzers via the CATC Sync Expansion Card

You can connect and control any of the following analyzers:

- ❑ SierraNet M408
- ❑ SierraNet M168
- ❑ Sierra FC M8-4
- ❑ Sierra FC M164

Select **File > New Project** to display the Add Device to Project dialog (see Figure 1.16 on page 13). Select the desired analyzer and click **OK**.



Device	Device Name	Location	Status	P1,P2	P3,P4	P5,P6	P7,P8
Sierra Net M408 SN: 64955	SierraGE_M168	172.16.129.125	Ready to connect	● 10GigE	● 10GigE	● 10GigE	● 10GigE
Sierra Net M408		Off-line		● 10GigE	● 10GigE	● 10GigE	● 10GigE
Sierra Net M168		Off-line		● 10GigE	● 10GigE	● 10GigE	● 10GigE
Sierra FC M164		Off-line		● FC	● FC	N/A	N/A
Sierra FC M8-4		Off-line		● FC	● FC	N/A	N/A

Select analyzer devices you want to connect

☑ Create new chain

Figure 1.16: Add Device to Project Dialog

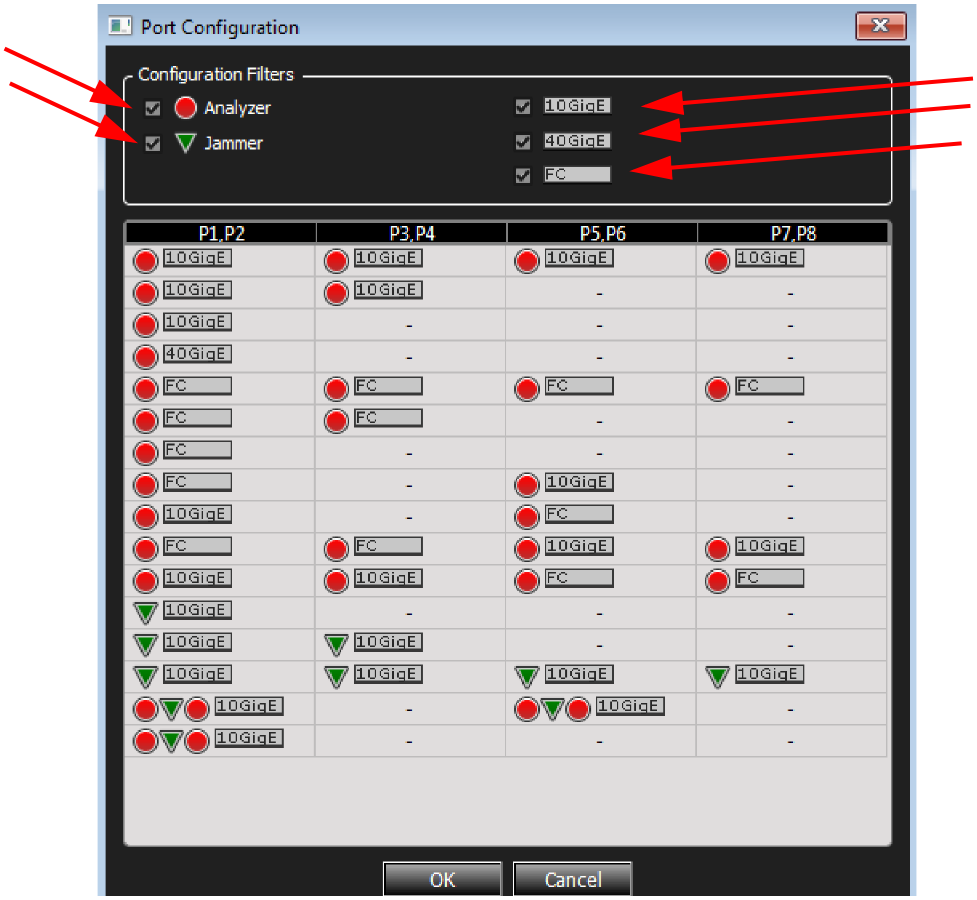
You can also create hybrid Ethernet/FC traces when the SierraNet M408 is daisy-chained with other compatible analyzers.

This is similar to the CrossSync functionality, but is done internal to the application, automatically.

You can connect to any of the off-line devices to create a dummy project and use the project when you are connected to a device.

You can select a function from Analyzer, Jammer or both, as well as the protocols you want to work with from 10 GigE, 40 GigE, FC or 10 GigE and FC by selecting the port pair combinations. Select the Device you want to connect to and click **More** to display the Port Configuration columns.

The software checks SFP speed for functional ports. If the software finds any mismatch between the given port configuration and SFPs, it displays a warning message describing the issues, but does not stop the Analyzer and/or Jammer.



Port Configuration

Configuration Filters

☑ ● Analyzer ☑ 10GigE
☑ ▽ Jammer ☑ 40GigE
☑ FC

P1,P2	P3,P4	P5,P6	P7,P8
● 10GigE	● 10GigE	● 10GigE	● 10GigE
● 10GigE	● 10GigE	-	-
● 10GigE	-	-	-
● 40GigE	-	-	-
● FC	● FC	● FC	● FC
● FC	● FC	-	-
● FC	-	-	-
● FC	-	● 10GigE	-
● 10GigE	-	● FC	-
● FC	● FC	● 10GigE	● 10GigE
● 10GigE	● 10GigE	● FC	● FC
▽ 10GigE	-	-	-
▽ 10GigE	▽ 10GigE	-	-
▽ 10GigE	▽ 10GigE	▽ 10GigE	▽ 10GigE
●▽● 10GigE	-	●▽● 10GigE	-
●▽● 10GigE	-	-	-

Figure 1.17: Port Configuration Dialog.

1.5 Launching Your Analyzer

To launch the software, double-click the Net Protocol Suite Icon in the Program Manager Window.

1.5.1 Using the Software

The SierraNet M408 application has protocol analysis software to capture data, trigger on Events, and save. Easy Mode allows standard Trigger and Data capture. Advanced Mode (see Figure 1.18 on page 15) allows you to program custom triggering, capturing, multi-state sequencing, and timers. (See “Protocol Analysis” on page 33.)

Switch to Advanced Mode Toggle Button

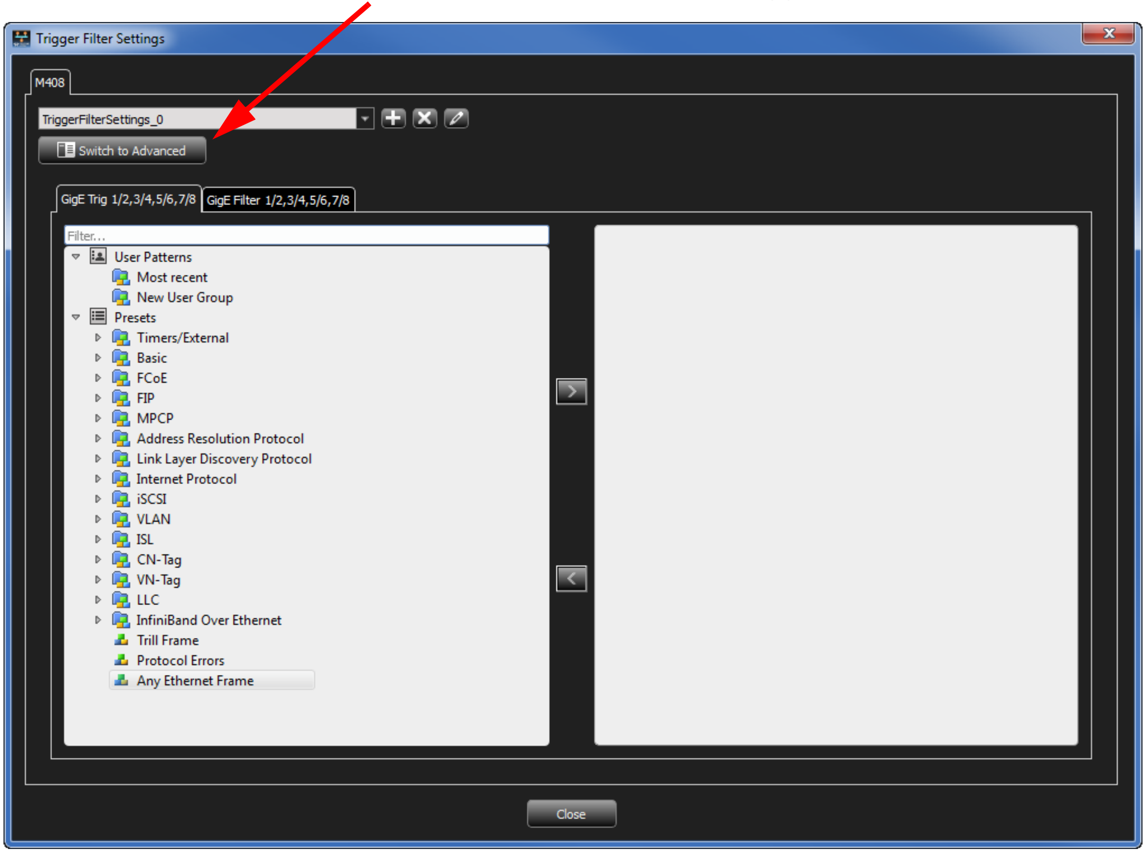


Figure 1.18: Easy/Advanced Mode Toggle Button.

1.5.2 Add Device to Project

After you start the software, select **File > New Project** to open Add Device to Project dialog. The following Add Device to Project dialog displays (see Figure 1.19 on page 16). The colors in the ‘Location’ column mean the following:

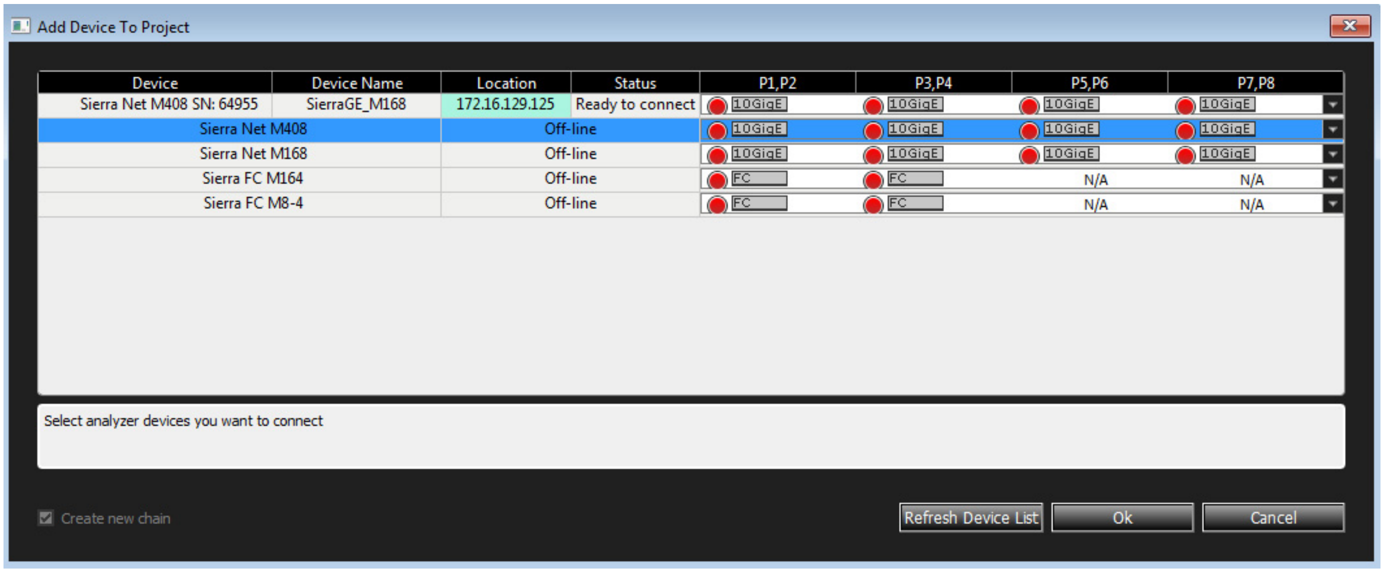
- ❑ Red: Device is not updated (firmware or one of bus engines is not updated).
- ❑ Light Blue: Ready to connect.
- ❑ Yellow: Device manually added and it is not connected OR device is locked.
- ❑ Green: Connected

Select a device with “Ready to connect” status.

If the device supports more than one protocol, select the desired protocols from the drop-down list in the Port column.

Select the port configuration from the Link Assignment column.

Click **OK** to connect to the device.



Device	Device Name	Location	Status	P1,P2	P3,P4	P5,P6	P7,P8
Sierra Net M408 SN: 64955	SierraGE_M168	172.16.129.125	Ready to connect	● 10GigE	● 10GigE	● 10GigE	● 10GigE
Sierra Net M408			Off-line	● 10GigE	● 10GigE	● 10GigE	● 10GigE
Sierra Net M168			Off-line	● 10GigE	● 10GigE	● 10GigE	● 10GigE
Sierra FC M164			Off-line	● FC	● FC	N/A	N/A
Sierra FC M8-4			Off-line	● FC	● FC	N/A	N/A

Select analyzer devices you want to connect

☑ Create new chain

Figure 1.19: Add Device to Project Dialog

Note: Click **Refresh Device List** to display all the devices on the on the local Ethernet subnet and also devices connected via USB cable.

1.5.3 Device Management

Click on **Setup** and select **Device Management** to open the Device Management dialog (see Figure 1.21 on page 17).

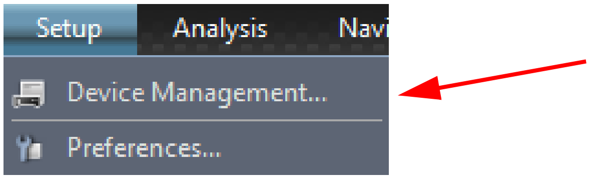
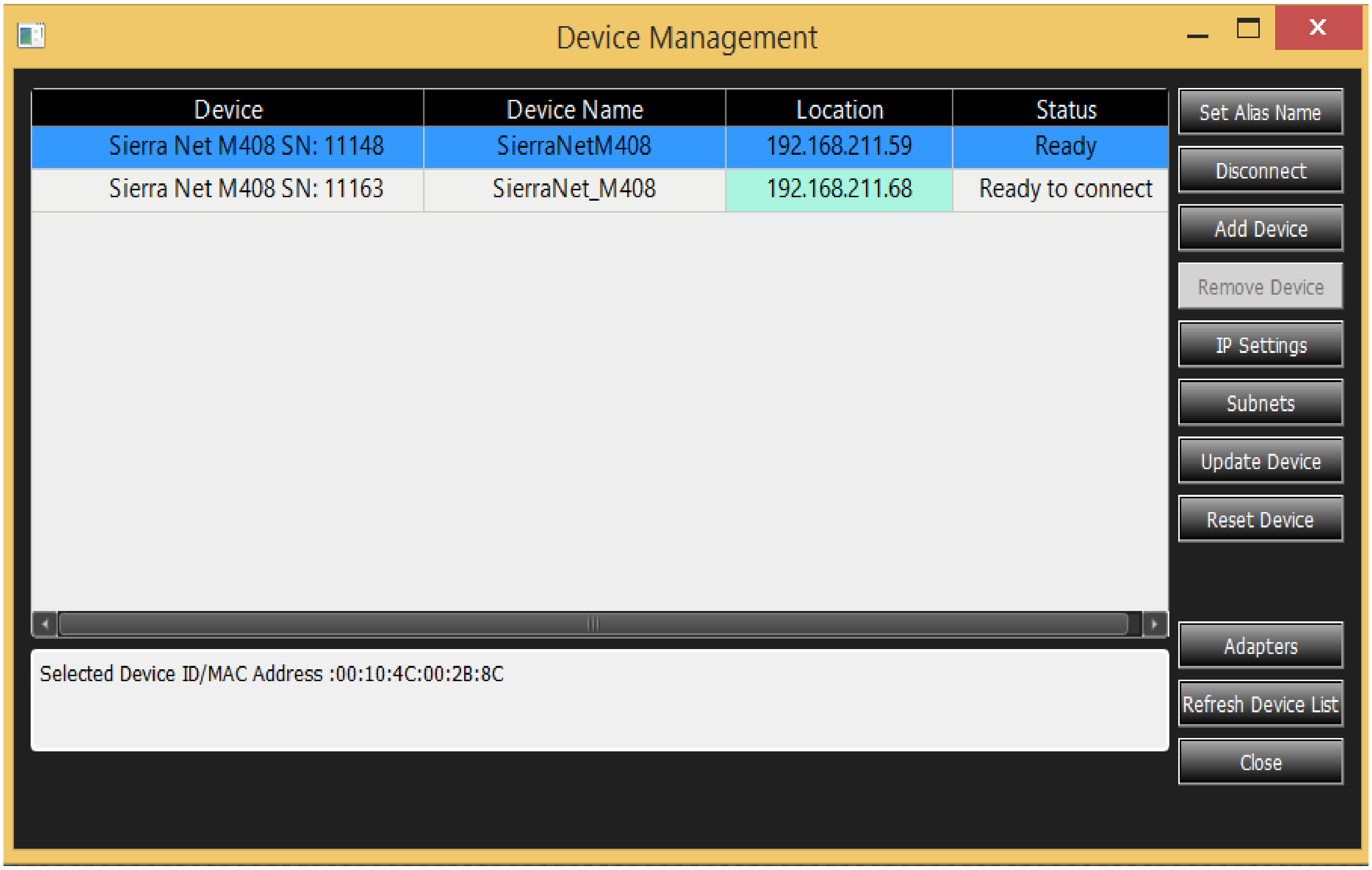


Figure 1.20: Connecting to Device(s).



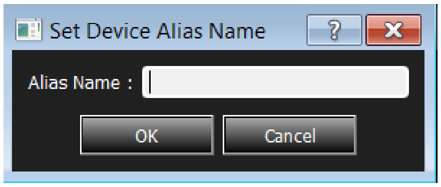
Device	Device Name	Location	Status
Sierra Net M408 SN: 11148	SierraNetM408	192.168.211.59	Ready
Sierra Net M408 SN: 11163	SierraNet_M408	192.168.211.68	Ready to connect

Selected Device ID/MAC Address :00:10:4C:00:2B:8C

Figure 1.21: Device Management Dialog.

Set Alias Name

Address Alias allows you to assign a meaningful name to each address to assist in interpreting the results displayed in the trace view. To assign address names in an open trace view, select **Setup > Device Management > Set Device Alias Name** (see Figure 1.22 on page 17.)



Alias Name :

Figure 1.22: Assign Alias Name.

Assign a meaningful name to each address in use and click **OK**. The assigned names replace the address in the trace view, Search, filter,. and Statistical Report.

If you elect to save the captured trace file, the assigned address names are saved together with the result, so that when you open the trace file later, the assigned names are retained.

Set As Default

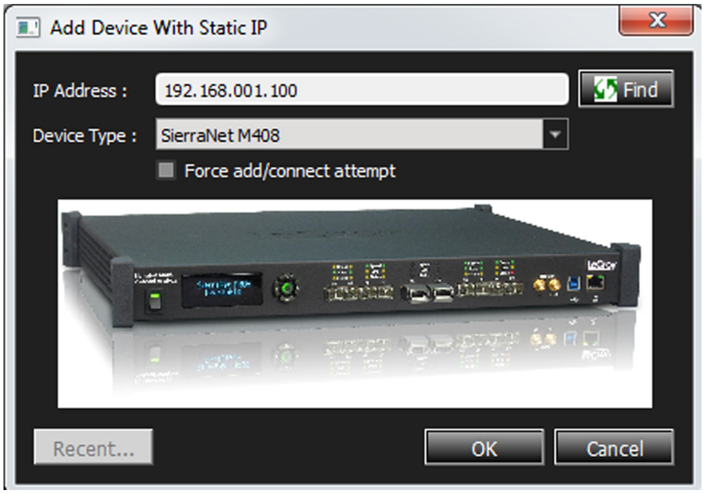
If you want to set these address aliases for trace files that will be captured later, you can set them as default, and new traces will be opened by these default address aliases.

Connect/Disconnect

Click **Connect** to connect or click **Disconnect** to disconnect a device.

Add Device...

Click **Add Device** to add a device with a static IP address.



IP Address : 192.168.001.100

Device Type : SierraNet M408

□ Force add/connect attempt

Figure 1.23: Add device.

Note: When entering addresses, you must include the leading zeros. Use 003.010.195.006 as entering 3.10.195.6 will not work. This is also applicable for Figure 1.33 on page 25.

Find

Click the **Find** button to test if the device at the specified IP address can be located.

Force Add/Connect Attempt

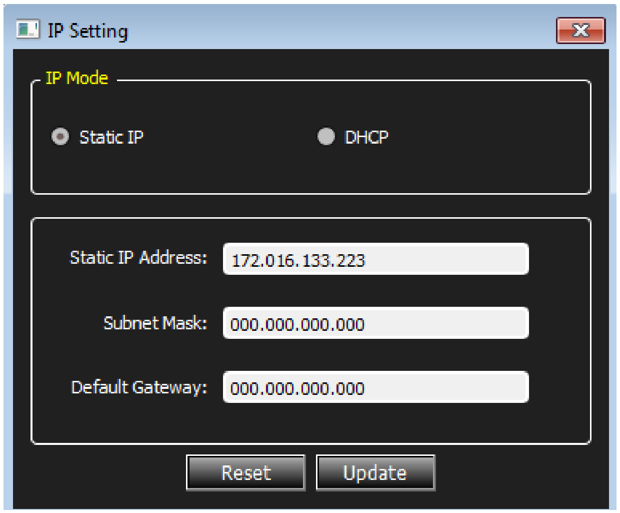
Use this option if the **Find** function fails, but you're sure the address is correct and you still want to attempt the connection. This setting is stored in the device list database and is applied when attempting to connect to the device.

Remove Device

Click **Remove Device** to remove a previously added device.

IP Settings

Click **IP Setting** to reset a device’s IP settings. The following IP Setting dialog displays (see Figure 1.24).


IP Setting

IP Mode

● Static IP ○ DHCP

Static IP Address: 172.016.133.223

Subnet Mask: 000.000.000.000

Default Gateway: 000.000.000.000

Figure 1.24: IP Setting Dialog.

Update Device

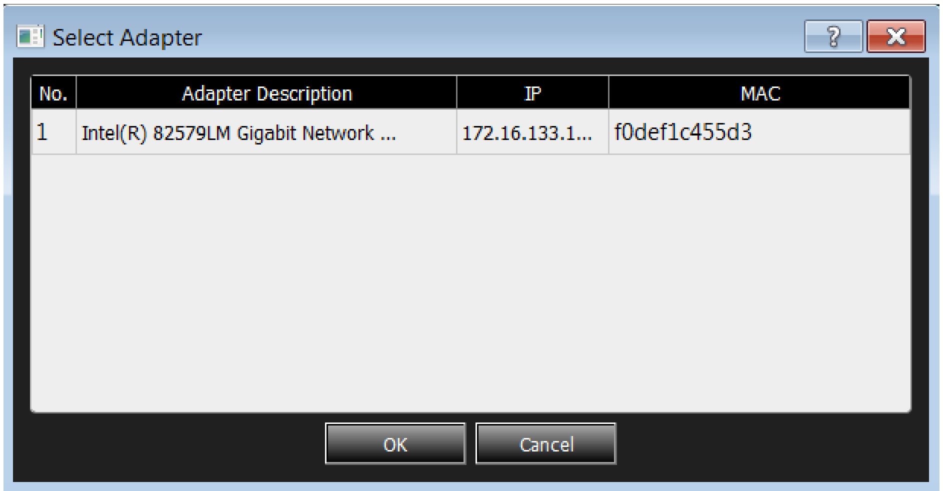
Click **Update** to update a device (see “Update Device” on page 28).

Subnets

Refer to section below (see “Ethernet Connectivity Through a Different Subnet” on page 22).

Adapters

Click **Adapters** to select the network adapter to use for connecting to Ethernet-connected devices. Some PCs have multiple adapters for connecting to different networks, so be sure to choose the one to which your desired device is connected. The following dialog displays.

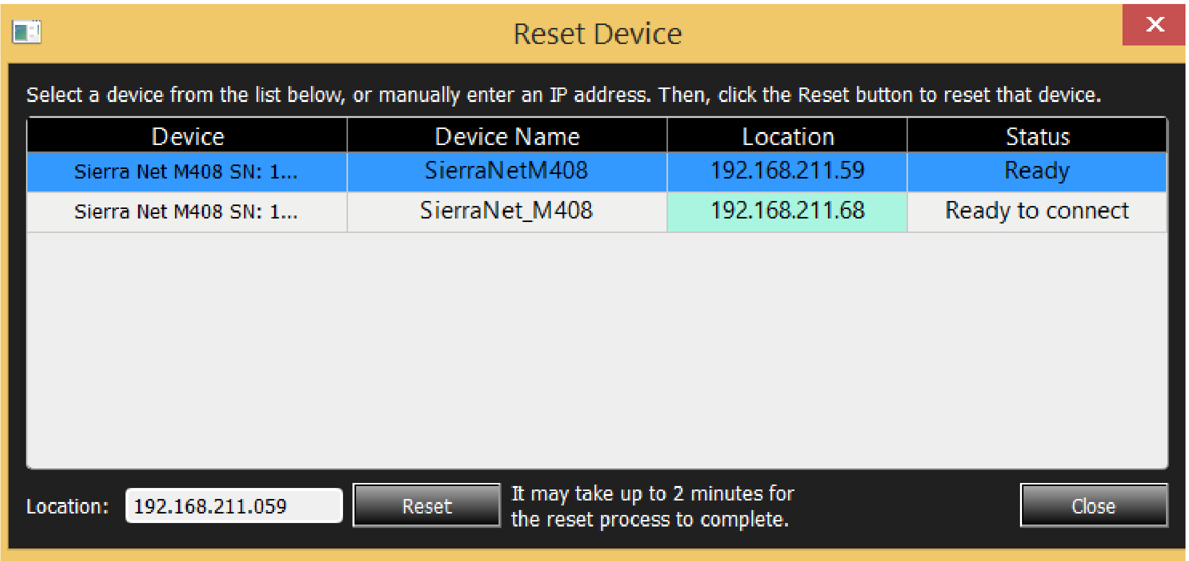

Select Adapter

No.	Adapter Description	IP	MAC
1	Intel(R) 82579LM Gigabit Network ...	172.16.133.1...	f0def1c455d3

Figure 1.25: Select Adapter Dialog.

Reset Device

Click **Reset Device** to open the Reset Device dialog. To Reset a Device, select a **Device** from the list below or enter an IP address. Then click the **Reset** button to reset the device.



Reset Device

Select a device from the list below, or manually enter an IP address. Then, click the Reset button to reset that device.

Device	Device Name	Location	Status
Sierra Net M408 SN: 1...	SierraNetM408	192.168.211.59	Ready
Sierra Net M408 SN: 1...	SierraNet_M408	192.168.211.68	Ready to connect

Location: 192.168.211.059

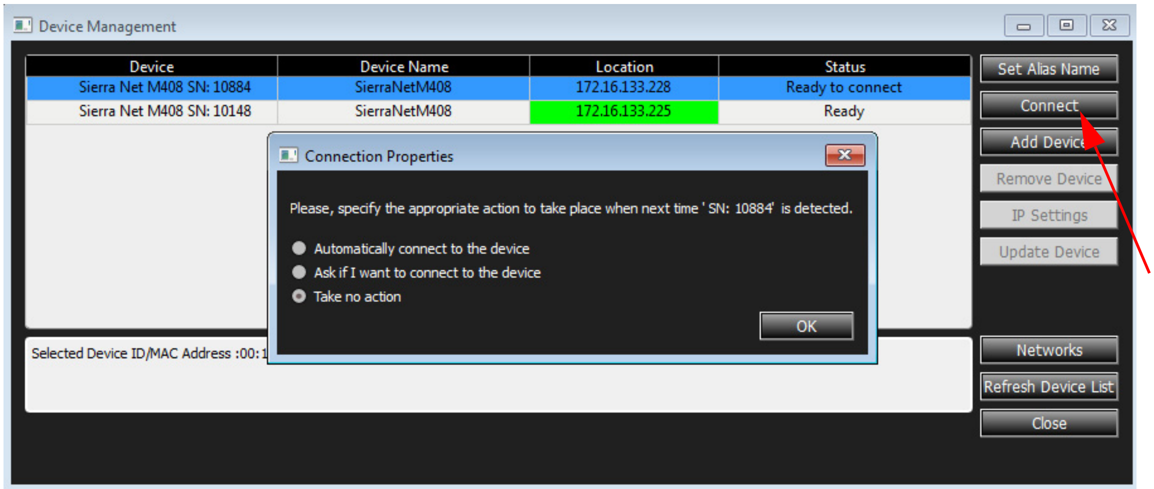
It may take up to 2 minutes for the reset process to complete.

Figure 1.26: Device Reset Menu

Refresh Device List

Click **Refresh Device List** to refresh the device list.

To connect to a device, select a device which is Ready to Connect and click the **Connect** button on the right. The Connection Properties dialog is displayed (see the following screen capture).



Device Management

Device	Device Name	Location	Status
Sierra Net M408 SN: 10884	SierraNetM408	172.16.133.228	Ready to connect
Sierra Net M408 SN: 10148	SierraNetM408	172.16.133.225	Ready

Selected Device ID/MAC Address :00:1

Connection Properties

Please, specify the appropriate action to take place when next time ' SN: 10884' is detected.

○ Automatically connect to the device
○ Ask if I want to connect to the device
● Take no action

Figure 1.27: Connection Properties Dialog.

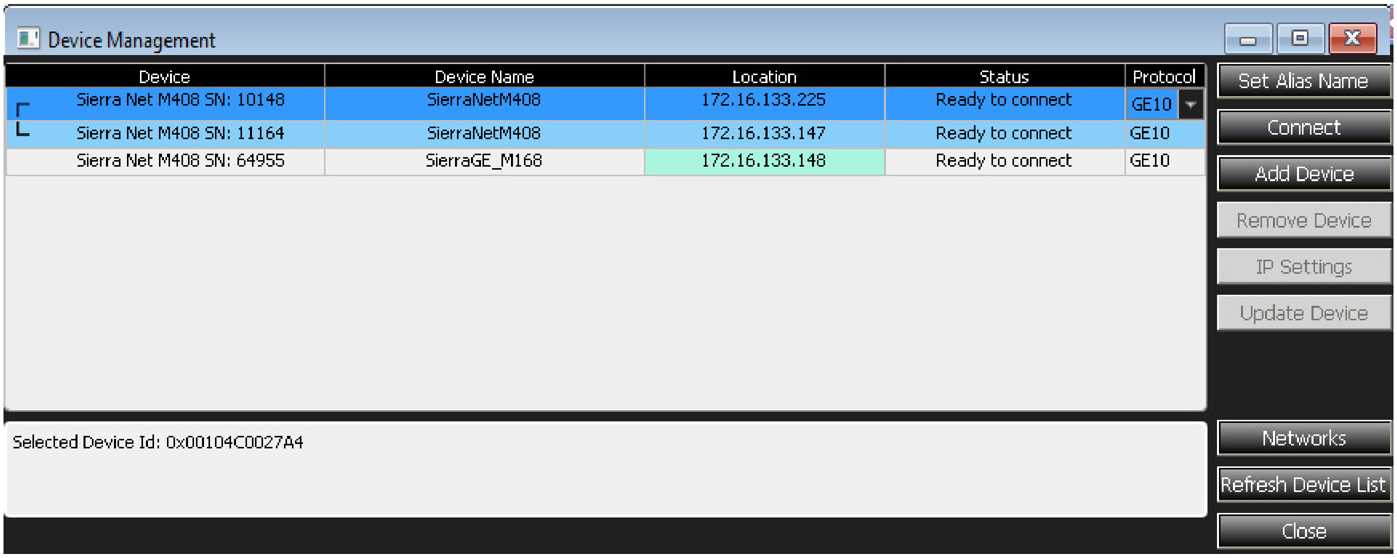
Specify one of the actions from the following:

- ❑ Automatically connect to the device
- ❑ Ask if I want to connect to the device

- ❑ Take no action

If ‘Automatically connect to the device’ is selected, the next time the application opens the device will be automatically connected.

In the **Device Management** dialog daisy-chained units are displayed in the **Device** column with a **[** (square bracket) icon. The sequence of the units is displayed in the **Order** column. See Figure 1.28.



Device	Device Name	Location	Status	Protocol
┌ Sierra Net M408 SN: 10148	SierraNetM408	172.16.133.225	Ready to connect	GE10
└ Sierra Net M408 SN: 11164	SierraNetM408	172.16.133.147	Ready to connect	GE10
Sierra Net M408 SN: 64955	SierraGE_M168	172.16.133.148	Ready to connect	GE10

Selected Device Id: 0x00104C0027A4

Figure 1.28: Device Management Dialog Displaying Unit 1 and Unit 2 Daisy-Chained together.

Note: When using the CATC Sync cards the order is automatically detected.

IMPORTANT! Power up all units before starting the software.

1.5.4 Connecting via Ethernet

The Ethernet connection can have any of these configurations:

1. Analyzer connected to the host computer (machine running the application software), using a switch, Gigabit Ethernet interface, or similar device.
2. Analyzer connected directly to the host computer using an Ethernet crossover cable.

To connect via USB refer to “Connecting Via USB” on page 27.

Connecting to a Network

When connected to a network, the analyzer can communicate with the DHCP server in order to obtain it's IP address configuration. The client needs to send a request to the DHCP server to obtain an IP. The server sends only one reply. The server does not necessarily send the available IP address

The SierraNet M408 product uses the following ports:
TCP Ports: 4000 - 4003

UDP Ports: 4033-4035

Connecting using a Switch, or Similar Device

The SierraNet M408 analyzer is automatically detected by the application if the analyzer and the host PC on which the application is running are on the same Ethernet subnet. If the analyzer and the host PC are located on different subnets then the IP address of the analyzer needs to be configured manually in the application. To add the IP address to the Select Device dialog, use the **Add Device** button (refer to “Add Device...” on page 18 and see Figure 1.24 on page 19). See Figure 1.24 on page 19 to set the IP address.

Analyzer Connected Directly to the Host Machine Using a Crossover Ethernet Cable

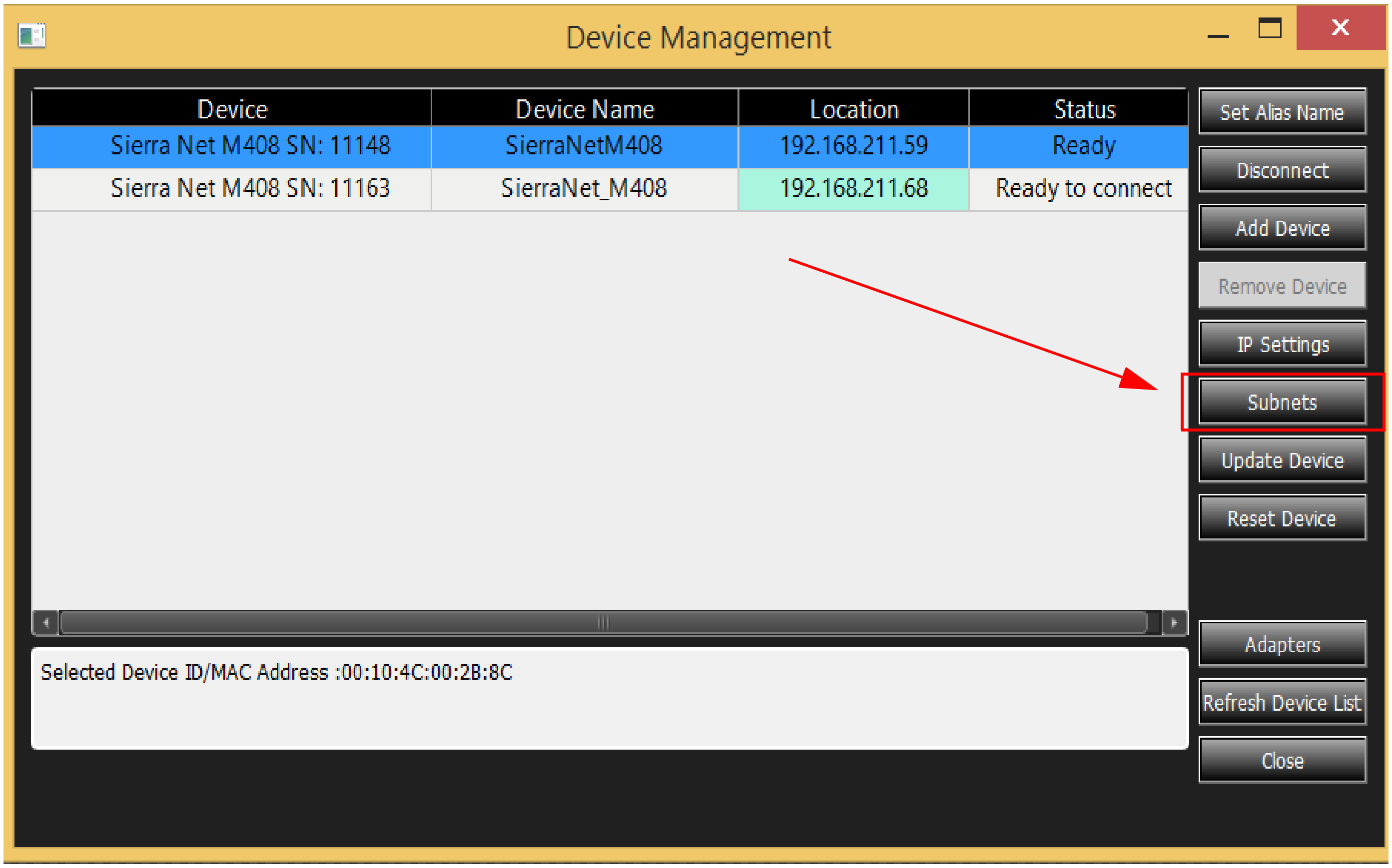
SierraNet M408 Systems are designed to connect to host PCs using a network connection, which allows the user to control the SierraNet M408 System from a local or remote host system. When connected to the host machine using a crossover ethernet cable, the Analyzer must be given a static IP address such that it will reside on the same subnet as the Ethernet interface of the host computer. See Figure 1.24 on page 19 to set the IP address.

Ethernet Connectivity Through a Different Subnet

The default discovery mechanism relies on broadcast messaging, which typically does not traverse between different subnets. Thus, alternate mechanisms are required to discover devices on different subnets. This section describes two methods: automatic subnet scanning and manual device adding.

Automatic Subnet Scanning

The software can be configured to automatically discover devices on other subnets. To do this, you must specify which subnets you would like the software to scan. This section describes how to add subnets so that the software will scan them for available devices.

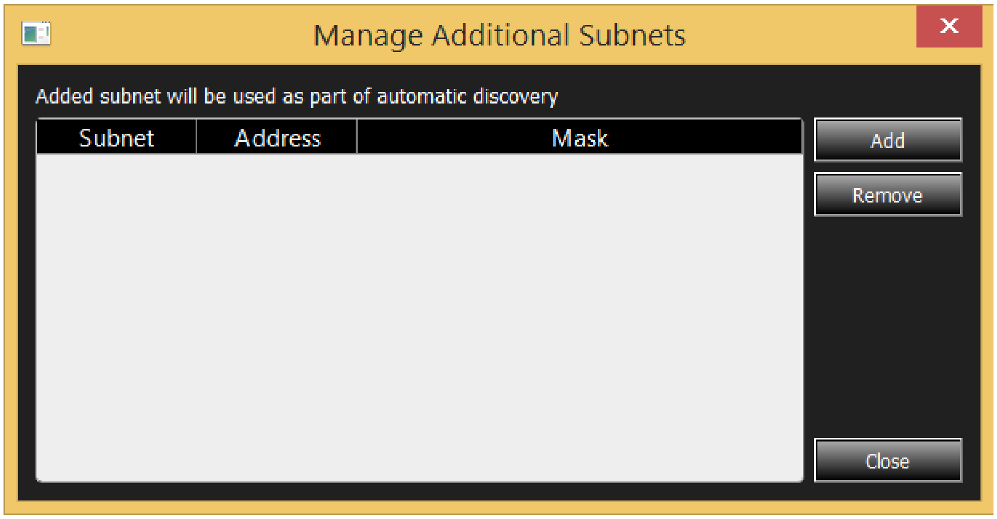


Device	Device Name	Location	Status
Sierra Net M408 SN: 11148	SierraNetM408	192.168.211.59	Ready
Sierra Net M408 SN: 11163	SierraNet_M408	192.168.211.68	Ready to connect

Selected Device ID/MAC Address :00:10:4C:00:2B:8C

Figure 1.29: Device List with Subnets Button

Clicking on the “Subnets…” button invokes the “Manage Additional Subnets” dialog, which shows the existing subnets and allows the user to add/remove them.

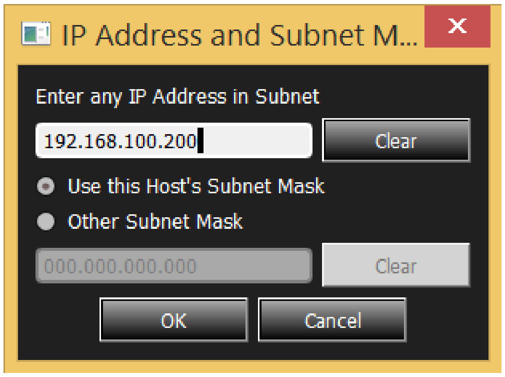


Added subnet will be used as part of automatic discovery

Subnet	Address	Mask

Figure 1.30: Manage Additional Subnets Dialog

Subnets in this list will be saved (e.g. to the Windows registry). Clicking on the “Add…” button invokes a dialog for adding another subnet.



Enter any IP Address in Subnet: 192.168.100.200

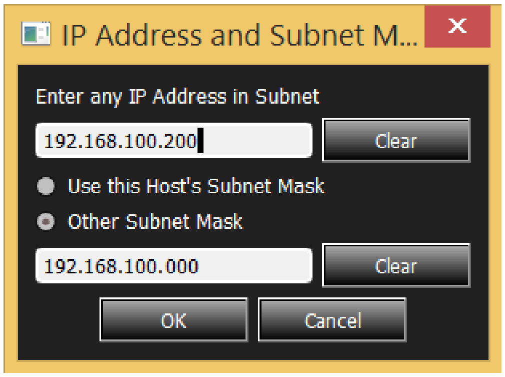
● Use this Host's Subnet Mask

○ Other Subnet Mask

000.000.000.000

Figure 1.31: Adding a Subnet with Host's Mask

A subnet is identified by a network IP address and a subnet mask, so both parameters must be specified. By default, we'll use the Host's subnet mask since it's most likely in enterprise environments that different subnets will still have the same mask. However, the option to provide some other subnet mask is provided.



Enter any IP Address in Subnet: 192.168.100.200

○ Use this Host's Subnet Mask

● Other Subnet Mask

192.168.100.000

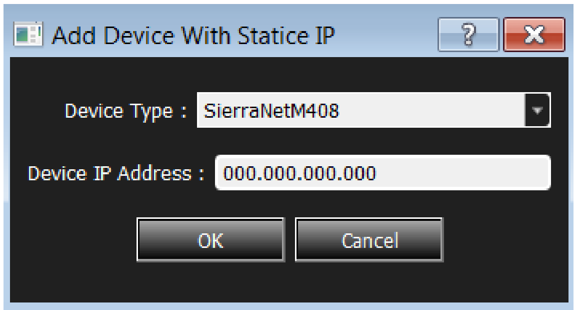
Figure 1.32: Adding a Subnet With a Different Mask

The software will validate the subnet to make sure it is not the same as the host's subnet.

Connecting Manually

If the device cannot be discovered through the automatic discovery mechanisms, you can discover it directly if you know its IP address. The SierraNet M408 IP address must be added manually. Perform the following steps:

1. Launch the application and click the Ethernet radio button.
2. Click **OK**.
3. Click **Add Device** in the Select Device dialog.
4. The Add Device with Static IP displays. Enter the IP address to add the device.



Device Type : SierraNetM408

Device IP Address : 000.000.000.000

Figure 1.33: Add New Device with Static IP Address

Once the IP address is added, the application will then send a connection request to that IP address to connect to the SierraNet M408 System.

Setup IP

This section describes the connectivity procedure for the SierraNet M408 System (see “IP Settings” on page 18).

Configuring the Ethernet Connection

There are two ways of configuring a SierraNet M408 for network connectivity:

- □ **DHCP** automatically assigns an IP address. DHCP is the default.
- □ **Static IP** prompts you to enter a specific IP address.

The SierraNet M408 can be configured from the unit itself using the five buttons and the LCD display on the front panel of the analyzer. For additional information, see “LCD Display and Button Functions for Configuring the Analyzer” on page 5.

Dynamic Configurations

Dynamic configuration uses DHCP (Dynamic Host Configuration Protocol).

Under DHCP, SierraNet M408 will issue a broadcast to any DHCP Server requesting configuration. If a DHCP server is present on the network, it will assign an IP address, Subnet Mask and a default GATEWAY (a router port IP address) to the SierraNet M408. The Gateway port will be used by SierraNet M408 to forward packets to IP addresses that do not reside within the same subnet.

When using the dynamic configuration, the front panel display will only update the IP address.

The subnet mask and gateway address will remain at the last values programmed

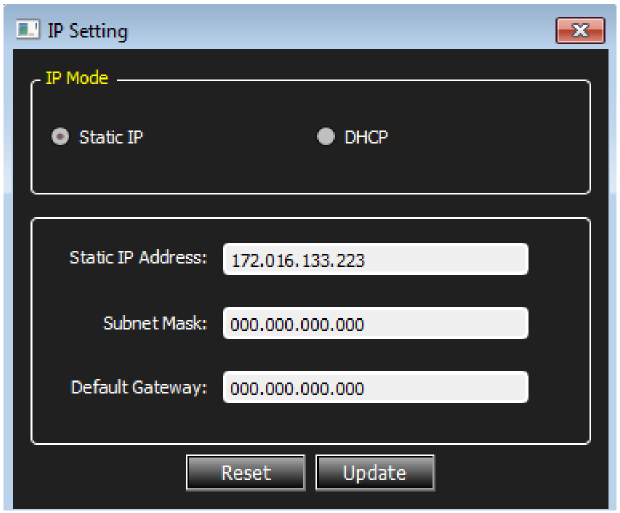
(000.000.000.000 by default, or whatever was last programmed in the static configuration). While in dynamic mode, these parameters will have actually been programmed within the IP STACK inside the SierraNet M408, but are not displayed in the LCD display.

To change from DHCP to Static IP, you must be connected to a device using USB:

1. Select **Setup > All Connected Devices > IP Settings** from the menu bar.

Note: If you are connected to the device using Ethernet, the Configuration menu does not have the Setup IP command.

The IP Setting dialog displays. For IP Mode, two radio buttons are available: Static IP and DHCP. DHCP is the default (see Figure 1.34 on page 26.)



● Static IP ○ DHCP

Static IP Address: 172.016.133.223

Subnet Mask: 000.000.000.000

Default Gateway: 000.000.000.000

Figure 1.34: Static IP Setup Dialog

Static Configurations

Within static configurations, SierraNet M408 must be manually programmed with an IP address, Subnet Mask and a default GATEWAY.

Once SierraNet M408 has been programmed with the static network configuration, it will broadcast a UDP message on its own subnet stating that is on line and available for connection.

Note: This broadcast is only on the subnet that includes the SierraNet M408 System.

When the application is started on the host machine, it will broadcast a UDP message on its own subnet asking all SierraNet M408s available to identify themselves.

Note: This broadcast is only on the host machine's subnet.

If the host machine and the SierraNet M408 System reside on the same subnet, they will see each other’s broadcasts and the application will automatically populate the Select Device list.

2. To change to Static IP, click the **Static IP** radio button.

   Enter the **Static IP Address**.

   Enter the **Subnet Mask**.

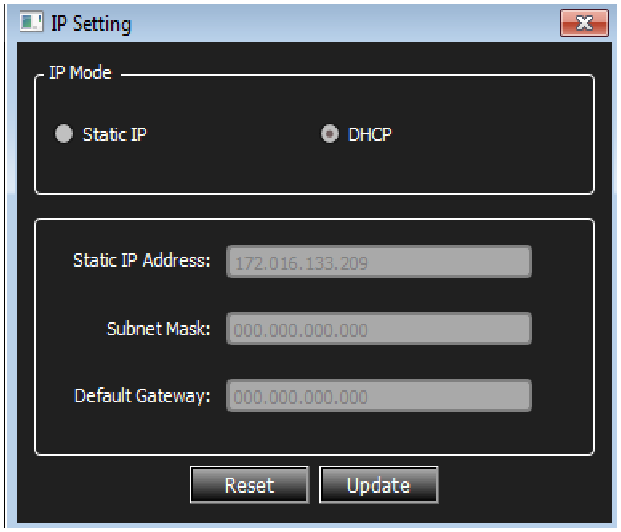
   Click **Update**.

   The system displays a warning message.

   Click **Yes** to get a success message.

Click **OK**. The message closes and the device resets.

3. To change back to DHCP, in the IP setup dialog, click the **DHCP** radio button, then click **Update.**



IP Setting

IP Mode

○ Static IP ● DHCP

Static IP Address: 172.016.133.209

Subnet Mask: 000.000.000.000

Default Gateway: 000.000.000.000

Figure 1.35: Dynamic IP Setup Success Message

After you see the Warning Message, click **Yes**

After you see the Success Message, click **OK**.

Note: You can also click **Reset**.

1.5.5 Connecting Via USB

To set up the Analyzer using a USB for the first time:

1. Remove the Analyzer from its shipping container.
2. Insert the Installation CD.
3. Connect the Analyzer to a power outlet using the provided power cord.
4. Connect the USB port to a USB port on the PC using a USB cable.
5. Turn on the rear power switch and the front power switch.
6. Click **Next** after you see the Add New Hardware Wizard dialog.
7. Follow the Microsoft® Windows® on-screen Plug-and-Play instructions for the automatic installation of the Analyzer as a USB device on your host machine. (The required USB files are included on the Installation CD.)
8. Click **Finish** when you see the message that says “Windows has finished installing the software that your new hardware requires” and the file has been installed in your host machine.

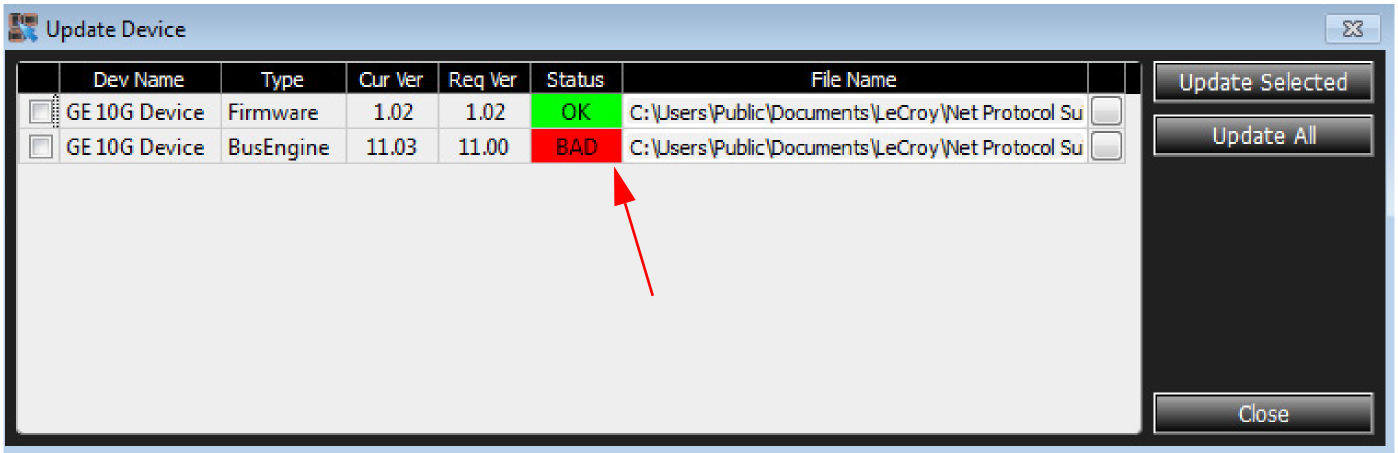
Note: Do not change from USB to Ethernet, or back, without power cycling the Analyzer.

To connect the Analyzer to a host system via ethernet, refer to "Connecting via Ethernet" on page 21.

1.5.6 Update Device

The Update Device dialog allows you to update the Firmware and BusEngine components of a connected analyzer. During the update process, the analyzer may reset and/or need to be power-cycled. Be sure to follow the on-screen prompts to complete the update process successfully.

1. Click the **Update Device** button on the Device Management dialog.



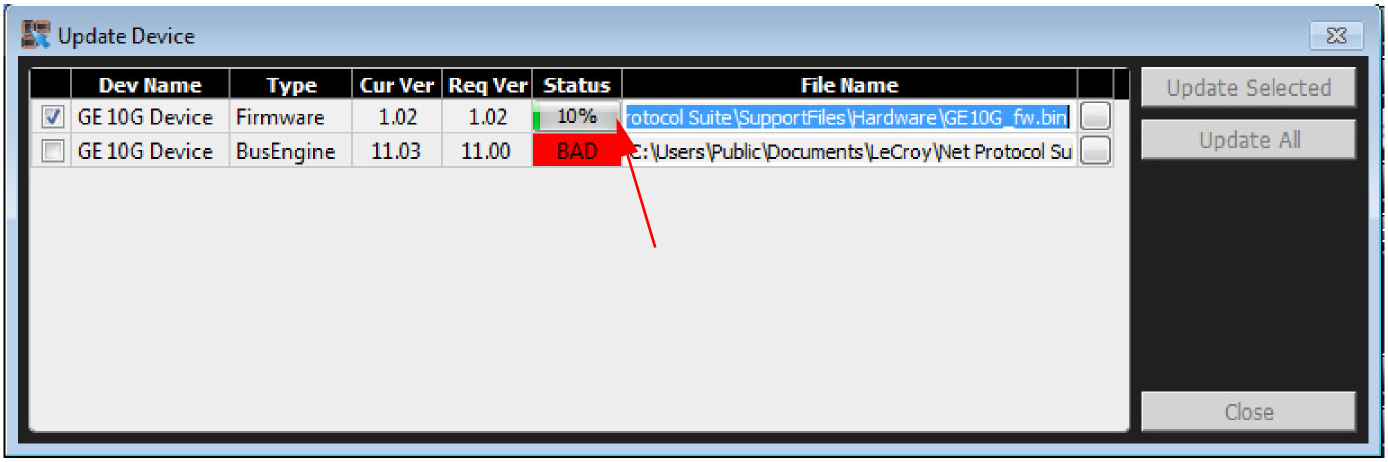
	Dev Name	Type	Cur Ver	Req Ver	Status	File Name
□	GE 10G Device	Firmware	1.02	1.02	OK	C:\Users\Public\Documents\LeCroy\Net Protocol Su
□	GE 10G Device	BusEngine	11.03	11.00	BAD	C:\Users\Public\Documents\LeCroy\Net Protocol Su

Figure 1.36: Update Device Dialog with a Bad Device Status

An item whose version is correct has an OK status in a green box.
An item whose version is mismatched has a BAD status in a red box.

Note: You can click the ellipses (...) at the end of a file path and name to display an Open dialog, in which you can browse for files.

2. Click the checkbox to the left of an item with BAD status, then click **Update Selected** to update that item to the correct version.



	Dev Name	Type	Cur Ver	Req Ver	Status	File Name
☑	GE 10G Device	Firmware	1.02	1.02	10%	otocol Suite\SupportFiles\Hardware\GE10G_fw.bin
□	GE 10G Device	BusEngine	11.03	11.00	BAD	C:\Users\Public\Documents\LeCroy\Net Protocol Su

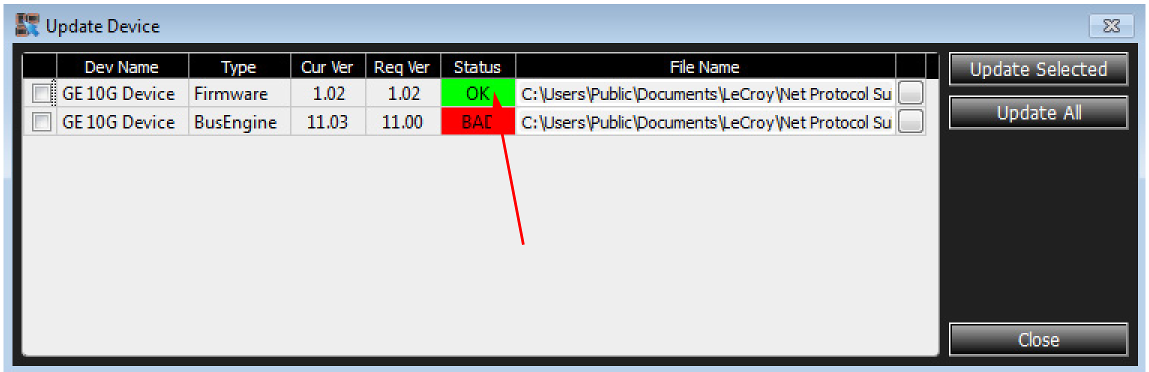
Figure 1.37: Update Device Dialog Beginning to Update Status of a Device

After the update, the device should restart. If the software prompts you to power-cycle the device, do so at this time; then the update will be complete.

Otherwise, when the software prompts you that the update is complete, the update process is done and you may continue using the device.

The connection may freeze when the unit reboots after the firmware update. Perform the following steps to recover:

1. Click **OK** on the error message in the Info dialog.
2. Click **Close** to close the Device Setup dialog.
3. Click **Refresh Device List** in the Device Management dialog (see Figure 1.28 on page 21).
4. Click **Disconnect**.



	Dev Name	Type	Cur Ver	Req Ver	Status	File Name	
□	GE 10G Device	Firmware	1.02	1.02	OK	C:\Users\Public\Documents\LeCroy\Net Protocol Su	□
□	GE 10G Device	BusEngine	11.03	11.00	BAD	C:\Users\Public\Documents\LeCroy\Net Protocol Su	□

Figure 1.38: Device Setup Dialog with OK Device Status

Note: Do not shut down or power cycle the analyzer during this process, unless specifically instructed to do so by the application.

1.6 Protocol Analyzer

To use the software for protocol analysis, first select **File > New Project** for a new project or **File > Open** to open an existing protocol analysis .gep file. (see “Protocol Analysis” on page 33.) You can also open a .get example file. Example files are in the Examples folder. You can also select **File > Recent Projects** to open a project you had recently saved.

Note: Select **File** from the main menu Analyzer Menu Bar or click on the **Hide Menubar** icon and select **File > Open.** Clicking the **Alt** key toggles showing/hiding the Analyzer Menu Bar.

Note: The application prevents the host machine from going into sleep mode to avoid loss of traces.

The software menus and toolbar options are explained in detail in “Software Menus and Toolbar” on page 36.

For more information on Analyzer Settings refer to “Analyzer Settings” on page 49.

1.6.1 Easy and Advanced Modes

The Easy Mode provides the quickest way to configure the analyzer to filter and trigger on events of interest. See “Trigger Filter Settings in Easy Mode” on page 64.

Use Advanced Mode only after you become familiar with the hardware and software and have special needs. To start working with the protocol analyzer and software. For more information on Advanced Mode refer to “Advanced Mode (User-Defined)” on page 104.

1.6.2 Viewing Captured Data

After data capture, the captured data is in the Viewer, see “Display Manipulation” on page 113. You can display the same data in:

- ❑ **Spreadsheet View**: Shows Protocol Fields and Frames by time.
- ❑ **Frame Inspector View:** Shows detail information about packet highlighted in Spreadsheet or Packet views.
- ❑ **Traffic Summary View:** The Traffic Summary View for each captured signal can be viewed. It displays errors for the whole trace or for a selected range. You can show grid lines, select rows and modify columns.
- ❑ **Data View:** The Data View displays information in Hexadecimal and ASCII format.

1.6.3 Preferences

For special work, you can use the Preferences menu to configure Software Settings, Port Alias, Address Alias and Display Settings. (See“Preferences” on page 149.)

1.6.4 Port Status

You can see an overview of the analyzer's ports in the Analyzer Settings Pane (see “Port Status Pane” on page 58).

1.7 InFusion

The Teledyne LeCroy InFusion™ Error Injector and Traffic Modifier is an error injector and traffic modification tool that allows you to verify real-world fault handling for SierraFC systems (see “InFusion” on page 163).

1.8 CrossSync Control Panel

The CrossSync Control Panel allows you to select analyzers for synchronization and manage the recording process. It supports a wide combination of Teledyne LeCroy’s flagship analyzers including PCI Express, USB, DDR, Serial ATA (SATA), Serial Attached SCSI (SAS), Fibre Channel (FC) and Ethernet.

CrossSync is Teledyne LeCroy’s analyzer synchronization solution that enables time-aligned display of protocol traffic from multiple daisy-chained analyzers showing packet traffic from multiple high-speed serial busses. A lightweight software control panel allows users to select analyzers for synchronization and manage the recording process. Captured traffic is displayed using the latest analyzer software (in separate windows) with all the protocol specific search and reporting features.

Captured packets are displayed in separate windows that share a common time scale. Navigating the traffic in either direction will scroll to the same timestamp in a synchronized window. When using the CrossSync option, users can access the full complement of analysis capabilities available within the individual Teledyne LeCroy software. Search, reporting, and decoding all operate normally.

This feature is available with the Teledyne LeCroy Net Protocol Suite software application.

1.8.1 Launching the CrossSync Control Panel

Click **Start > Programs > LeCroy > CrossSync > CrossSync Control Panel** to launch the application.

Chapter 2

Protocol Analysis

The system performs Protocol Analysis by defining and running an analysis project for both Fibre Channel over Ethernet (FCoE) and Fibre Channel (FC) depending on the Analyzer that you are connected to. A captured trace is saved in a file with the **.get** extension. An analysis project definition defines what to capture, what the analyzer triggers on, and the memory settings. You can save defined projects as project ***.gep** files for later use.

After you install the Analyzer software (see "Software Installation" on page 7) and set up the Analyzer (see "Hardware Setup" on page 7), launch the Analyzer software (see "Launching Your Analyzer" on page 14) to display the main window.

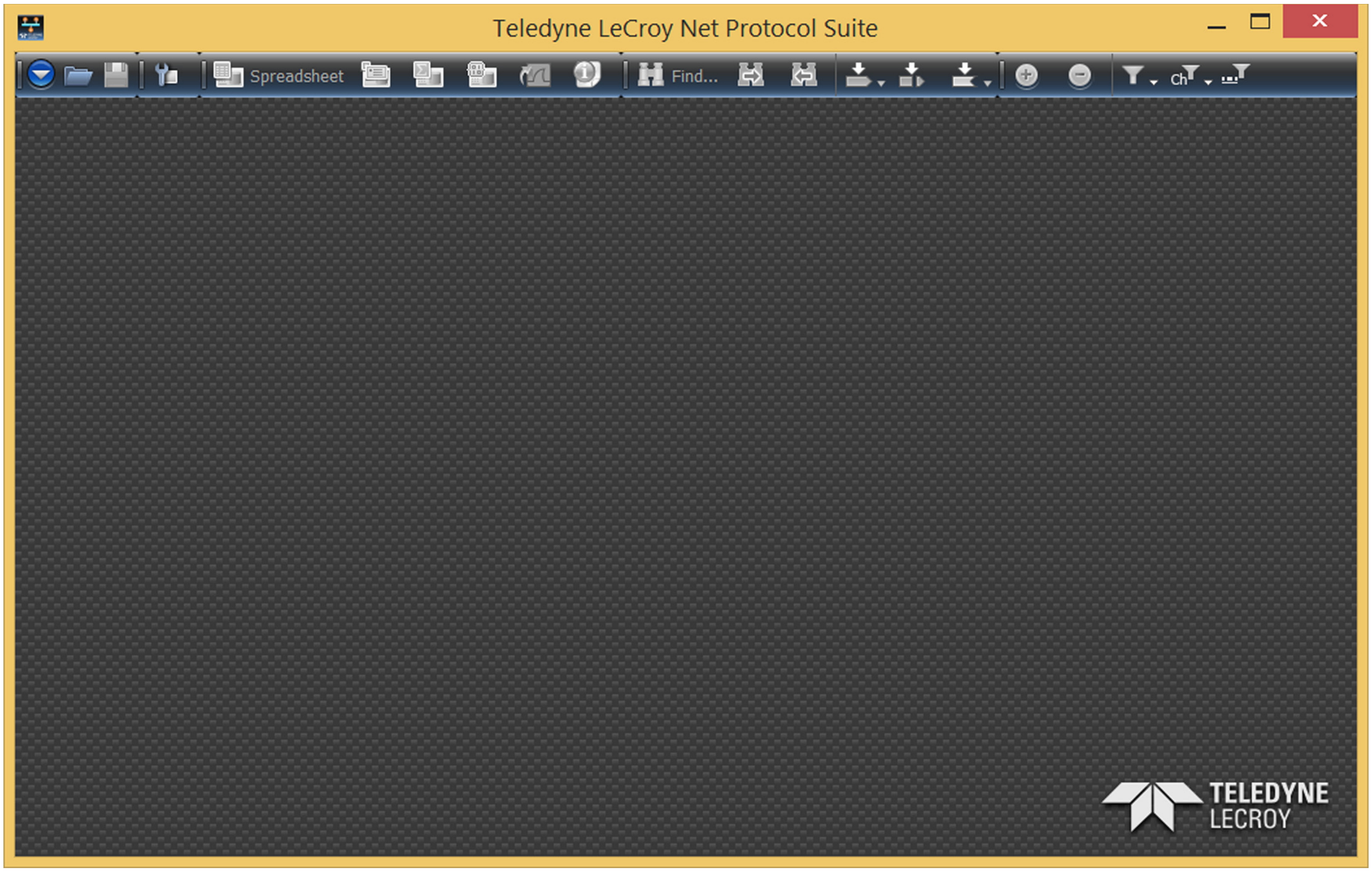


Figure 2.1: Teledyne LeCroy Ethernet Protocol Suite Main Window.

2.1 Starting a New Project

To start a new project, click **File > New Project** from the Analyzer menu options, or click on the **Hide Menubar** icon and select **File > New Project** (see Figure 2.2) to display the Add Device to Project dialog (see Figure 1.16 on page 13). Select the desired analyzer and click **OK.**

Note: Click **Alt** to toggle between showing/hiding the top menu bar.

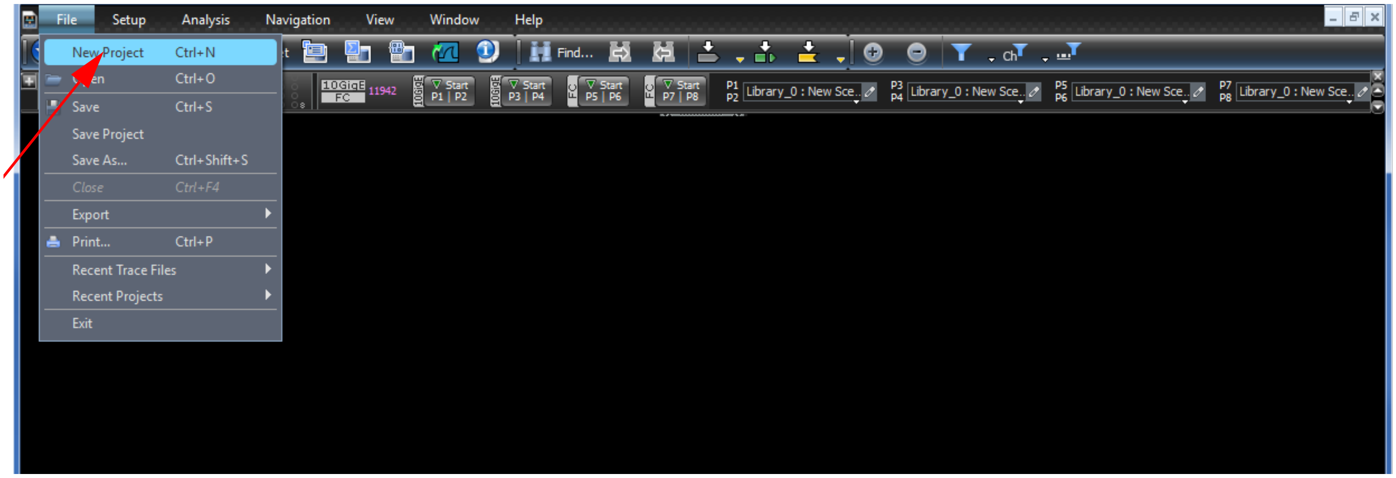


Figure 2.2: Starting a New Project from the Application Menu bar

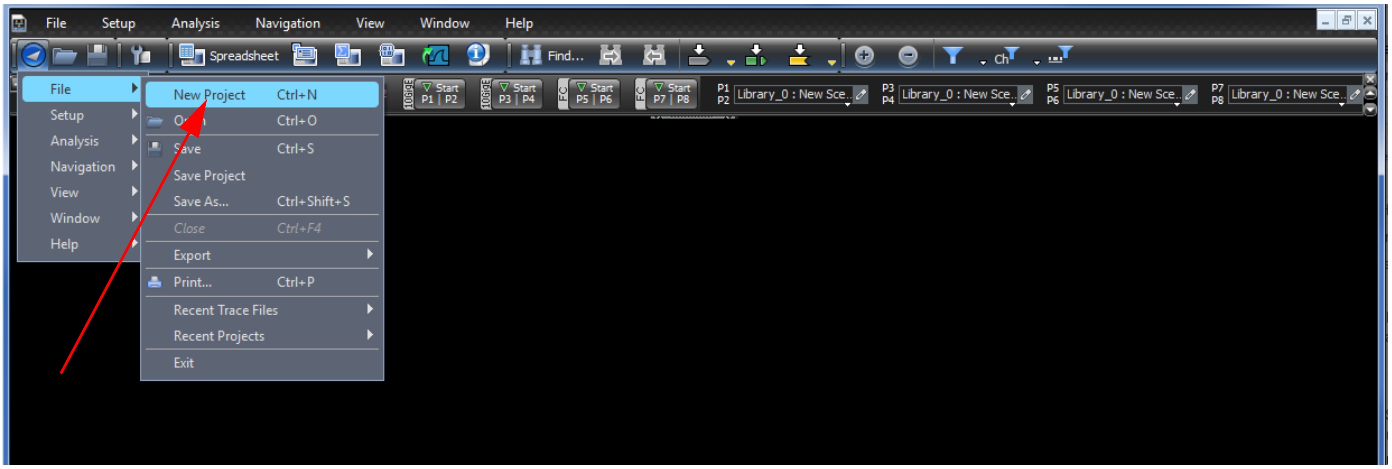


Figure 2.3: Starting a New Project from the Menu button on the Application toolbar

The New Project main window opens with default settings to capture Everything on the bus and to Trigger On on Snapshot. (The analyzer captures everything immediately without triggering on anything in particular.)

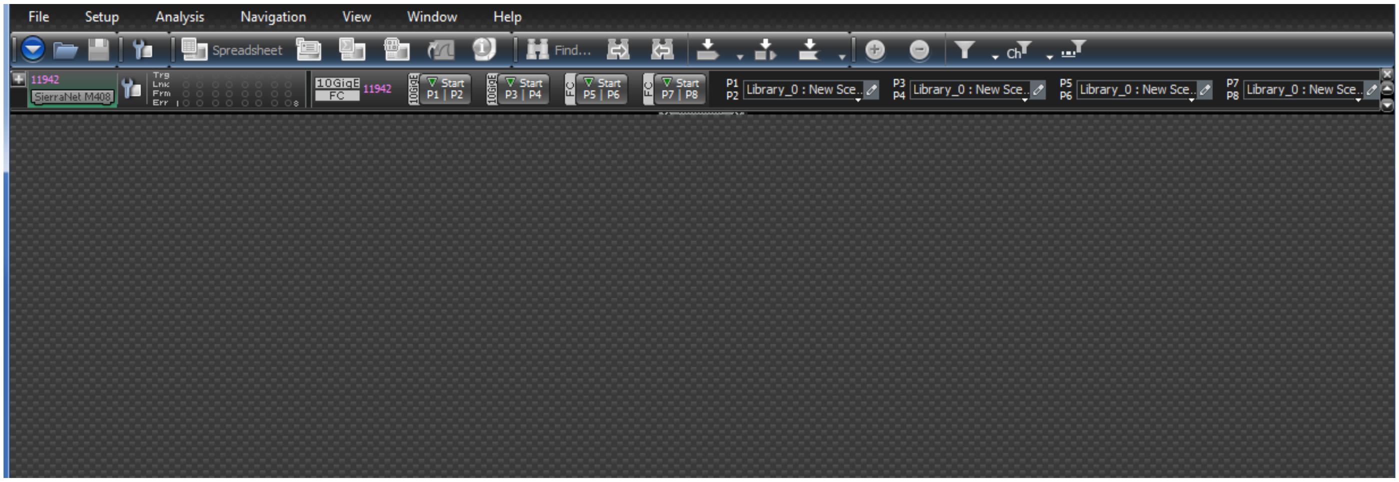


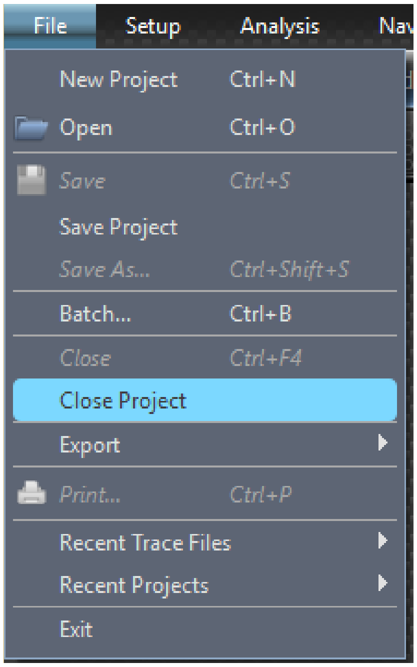
Figure 2.4: Main Window.

2.2 Opening an Existing Project

To open an existing project, click **File > Open** from the Analyzer Menu Bar to open an existing .gep project, or click on the **Hide Menubar** icon and select **File > Open**.

2.3 Closing an Existing Project

Close Project allows you to close the current project without closing the Protocol Suite.



2.4 Software Menus and Toolbar

The menu toolbar options are given in the following table.

	Open icon. Click to open a file. See “File” on page 38.
📂	Open icon. Click to open a file. See “File” on page 38.
💾	Save icon. Click to save a file. See “File” on page 38.
	Preferences icon. Click to save a file. See “Preferences” on page 40.
Spreadsheet	Spreadsheet View icon. See “Spreadsheet View” on page 118.
	Frame Inspector View icon. See “Frame Inspector View” on page 128.
	Traffic Summary icon. See “Traffic Summary View” on page 43.
	Data View icon. See “Data View” on page 43.

	Export to Wireshark icon. Click to export trace to Wireshark and launch the Wireshark application. Wireshark must be installed on the PC. Wireshark is a free application available at www.wireshark.org. (see “Export and Open with Wireshark” on page 39).
	Displays the Trace information dialog. (see “Trace Information” on page 44).
	Find icon. You can search for specific Triggers and specify the From, Domain, Direction and Logic. See “Find” on page 144.
	Find Next icon. Searches for the next instance.
	Find Previous icon. Searches for the previous instance.
	Go to icon. Click to locate cursors or specific packets: Timestamp, X Position, Y Position, Event, Begin, and End. See Figure 2.17 on page 47.
	Go to Trigger icon. Click to go to the trigger point in the trace. See Figure 2.17 on page 47.
	Go to Marker icon. Click to go to a specific Marker. See “Markers” on page 127.
	Zoom in icon. Searches for the previous instance.
	Zoom out icon. Searches for the previous instance.
	Filter icon. Click to open the filter dialog. See “Filtering” on page 138.
Ch	Ports icon. Click to select a port. See “Ports” on page 135.
	Idles icon. Click to show/hide idles in a trace.
	Device External Trig Setting icon. Click to open the Device Settings dialog. See “External Trigger” on page 58.
	Recording Setting icon. Click to open the Recording Setting dialog. See “Recording Settings Pane” on page 59.
	Trigger Filter Settings icon. Click to open the Trigger Filter Settings dialog. See “Patterns and Data Capture Setup” on page 71.

2.5 Application Menu Options

The following menu options display in the main window:

- File
- Setup
- Analysis
- Navigation
- View
- Window
- Help

2.5.1 File

The File menu has the standard menu options as shown in the following screen capture.

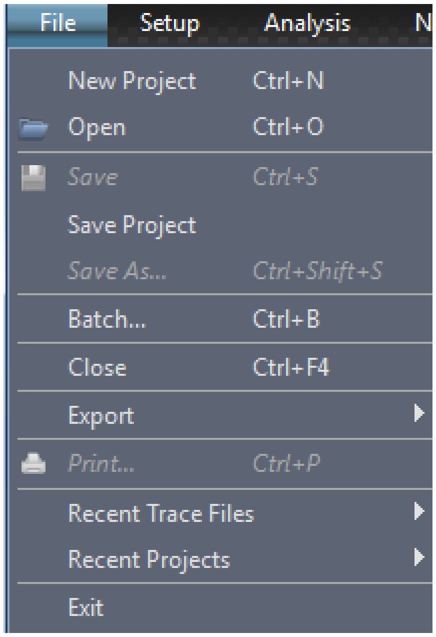


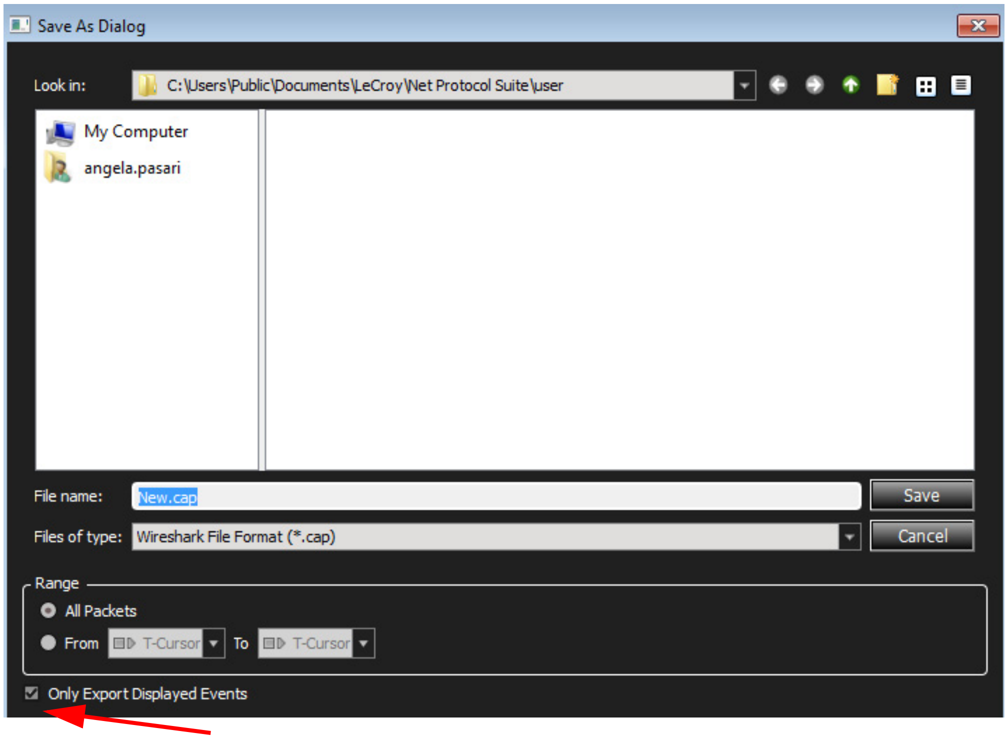
Figure 2.5: File Menu Options.

New Project	Click to open a new project.
Open	Click to open an existing trace or trace files.
Save	Click to save an existing trace or trace files.
Save Project as	Click to save the current project with a different name or directory.
Save as	Click to save an existing trace or trace files with a different name or directory.
Batch	Click to run batch scenarios. (see "Batch Scenario" on page 217). Available only after a project is open.
Close	Click to close a frame or window when multiple frames or windows are open.

Export	Export file to Excel, text or export and open with Wireshark (see “Export and Open with Wireshark” on page 39)
Print/Print Preview/Print Setup	Printing options for the file
Recent Trace Files	Lists recent trace files to open
Recent Projects	Lists recent projects to open
Exit	Click to exit the application.

Export and Open with Wireshark

Selecting **File** > **Export and Open with Wireshark** or clicking the icon displays the Save As Dialog. Checking the Only Export Displayed Events box exports only the displayed events. If the box is unchecked, then all the contents of the trace file are exported. Only Ethernet content is exported; Fibre Channel content is not exported.



Save As Dialog

Look in: C:\Users\Public\Documents\LeCroy\Net Protocol Suite\user

My Computer

angela.pasari

File name: New.cap

Files of type: Wireshark File Format (*.cap)

Range

● All Packets

○ From T-Cursor To T-Cursor

☑ Only Export Displayed Events

Figure 2.6: Wireshark Save As Dialog.

2.5.2 Setup

The Setup menu has the following options to setup and configure the device:

- Device Management
- Preferences

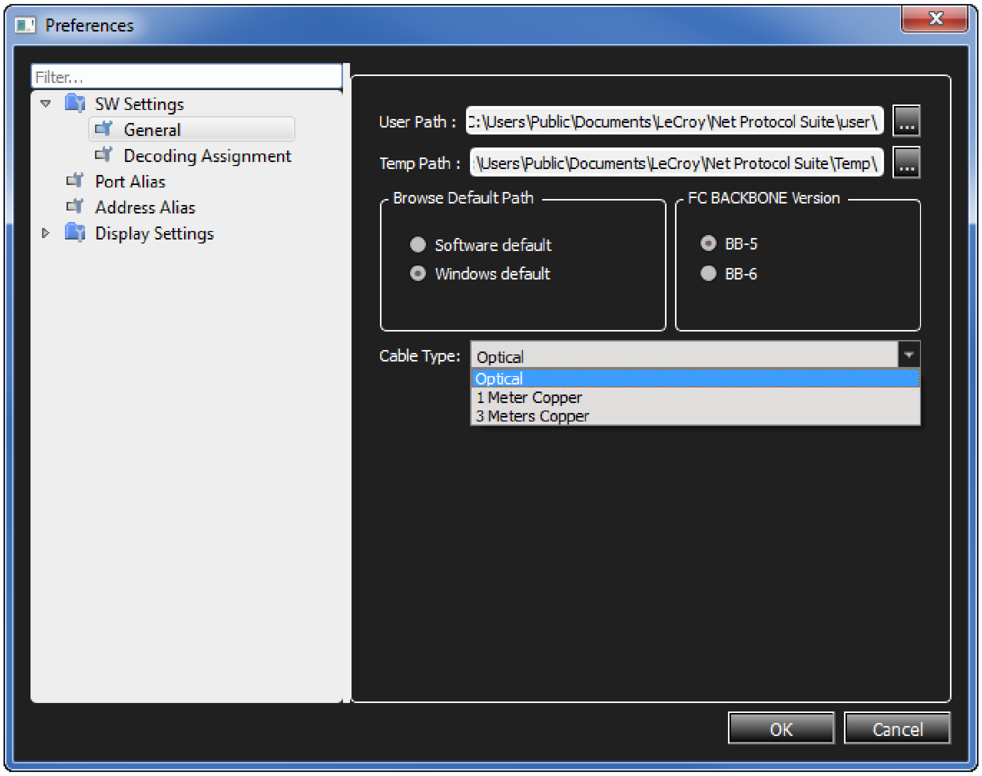
Device Management

Click **Device Management** to display the Device Management dialog. Refer to "Device Management" on page 16 for more information.

Preferences

The Preferences option allows you to set the software and display settings.

Click on **Setup > Preferences** or click icon to display the Preferences dialog (see Figure 2.7 on page 40) and configure these settings. Refer to "Preferences" on page 149 for more information.



User Path : C:\Users\Public\Documents\LeCroy\Net Protocol Suite\user\

Temp Path : \Users\Public\Documents\LeCroy\Net Protocol Suite\Temp\

Browse Default Path
○ Software default
● Windows default

FC BACKBONE Version
● BB-5
○ BB-6

Cable Type: Optical

Figure 2.7: Preferences Dialog.

The following can be configured in Preferences:

- Software Settings
- Port Alias
- Address Alias
- Display settings
- User Path
- Temp Path
- Browse Default Path
  - Software default
  - Windows default
- FC Backbone Version
  - BB-5
  - BB-6

2.5.3 Analysis

The Analysis menu has the following options to view trace files and specify SCSI decoding assignments:

- ❑ Decoding Assignments
- ❑ Spreadsheet View
- ❑ Frame Inspector View
- ❑ Traffic Summary View
- ❑ Data View
- ❑ Trace Information

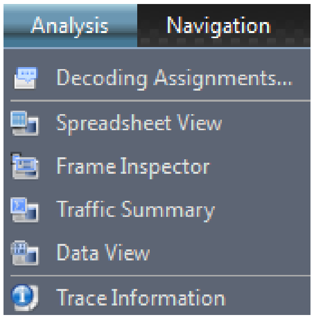
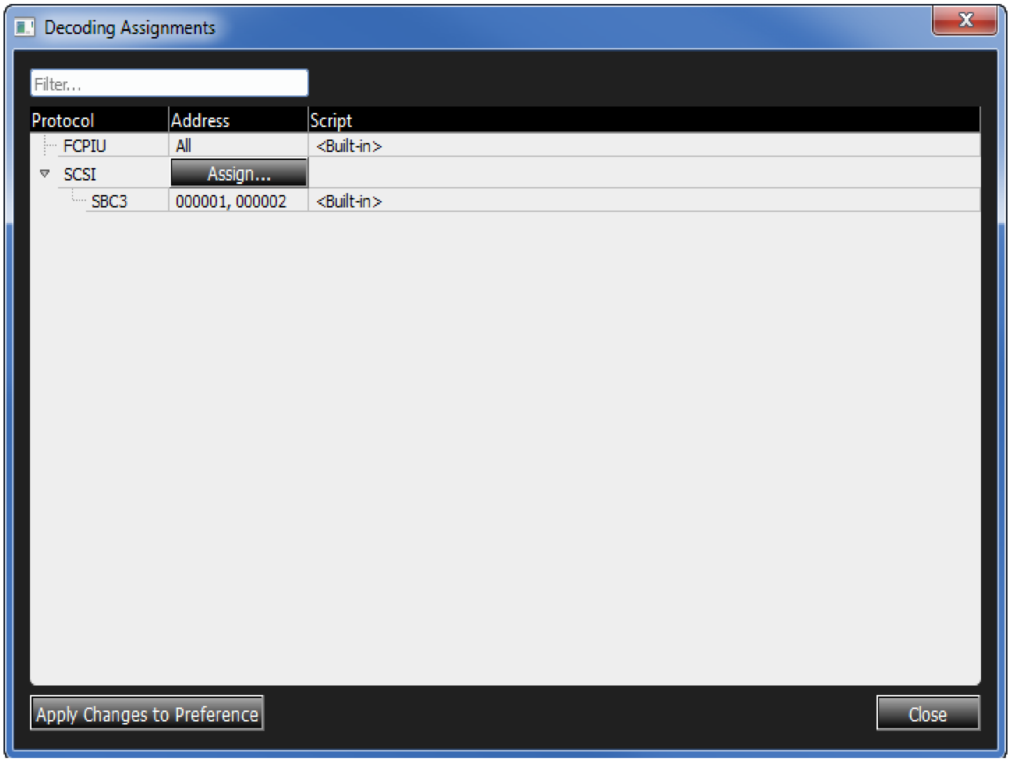


Figure 2.8: Analysis Menu.

Decoding Assignments

Click on **Analysis** and select **Decoding Assignments** to display the **Decoding Assignments** dialog.

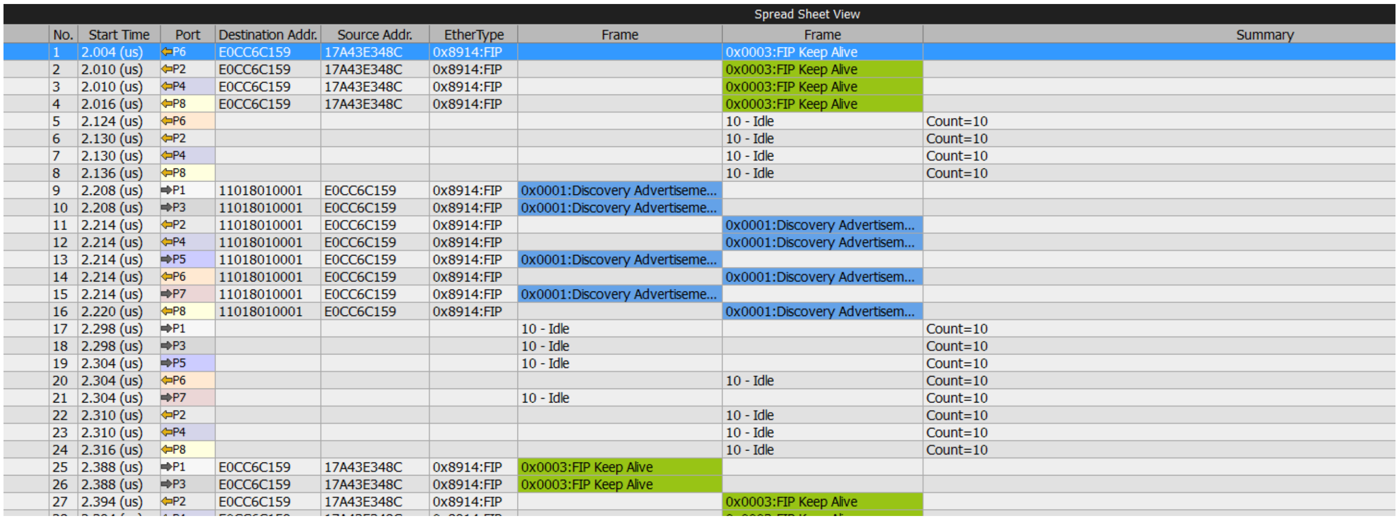


Protocol	Address	Script
FCPIU	All	<Built-in>
SCSI	Assign...	
SBC3	000001, 000002	<Built-in>

Figure 2.9: Decoding Assignments Dialog.

Spreadsheet View

Click on **Analysis** and select **Spreadsheet View** or click the Spreadsheet icon to display the Spreadsheet View.



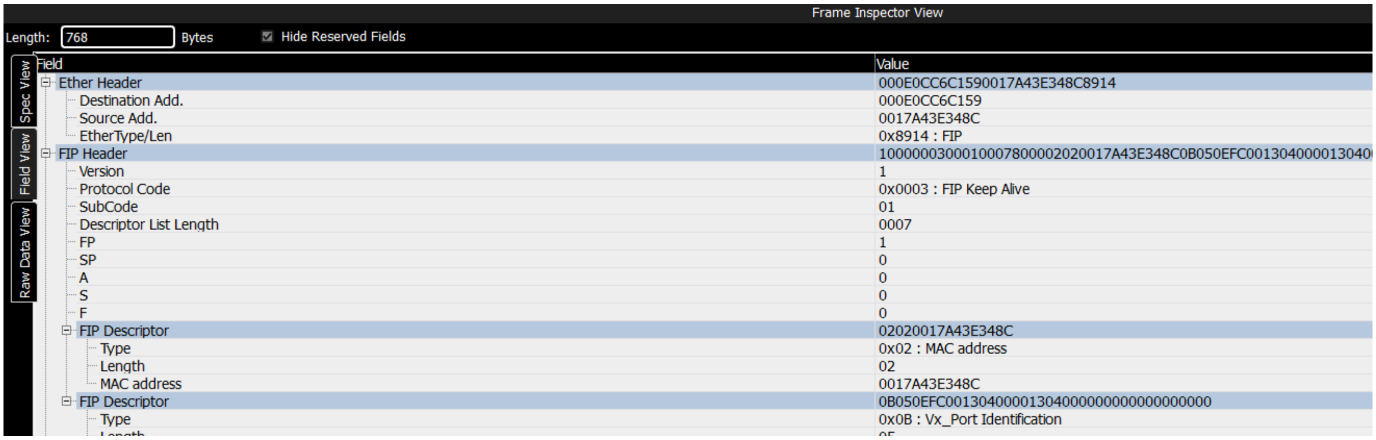
No.	Start Time	Port	Destination Addr.	Source Addr.	EtherType	Frame	Frame	Summary
1	2.004 (us)	⇦P6	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	
2	2.010 (us)	⇦P2	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	
3	2.010 (us)	⇦P4	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	
4	2.016 (us)	⇦P8	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	
5	2.124 (us)	⇦P6					10 - Idle	Count=10
6	2.130 (us)	⇦P2					10 - Idle	Count=10
7	2.130 (us)	⇦P4					10 - Idle	Count=10
8	2.136 (us)	⇦P8					10 - Idle	Count=10
9	2.208 (us)	➡P1	11018010001	E0CC6C159	0x8914:FIP	0x0001:Discovery Advertiseme...		
10	2.208 (us)	➡P3	11018010001	E0CC6C159	0x8914:FIP	0x0001:Discovery Advertiseme...		
11	2.214 (us)	⇦P2	11018010001	E0CC6C159	0x8914:FIP		0x0001:Discovery Advertisem...	
12	2.214 (us)	⇦P4	11018010001	E0CC6C159	0x8914:FIP		0x0001:Discovery Advertisem...	
13	2.214 (us)	➡P5	11018010001	E0CC6C159	0x8914:FIP	0x0001:Discovery Advertiseme...		
14	2.214 (us)	⇦P6	11018010001	E0CC6C159	0x8914:FIP		0x0001:Discovery Advertisem...	
15	2.214 (us)	➡P7	11018010001	E0CC6C159	0x8914:FIP	0x0001:Discovery Advertiseme...		
16	2.220 (us)	⇦P8	11018010001	E0CC6C159	0x8914:FIP		0x0001:Discovery Advertisem...	
17	2.298 (us)	➡P1				10 - Idle		Count=10
18	2.298 (us)	➡P3				10 - Idle		Count=10
19	2.304 (us)	➡P5				10 - Idle		Count=10
20	2.304 (us)	⇦P6					10 - Idle	Count=10
21	2.304 (us)	➡P7				10 - Idle		Count=10
22	2.310 (us)	⇦P2					10 - Idle	Count=10
23	2.310 (us)	⇦P4					10 - Idle	Count=10
24	2.316 (us)	⇦P8					10 - Idle	Count=10
25	2.388 (us)	➡P1	E0CC6C159	17A43E348C	0x8914:FIP	0x0003:FIP Keep Alive		
26	2.388 (us)	➡P3	E0CC6C159	17A43E348C	0x8914:FIP	0x0003:FIP Keep Alive		
27	2.394 (us)	⇦P2	E0CC6C159	17A43E348C	0x8914:FIP		0x0003:FIP Keep Alive	

Figure 2.10: Spreadsheet View.

Spreadsheet View displays Protocol Fields and Frames by time. Refer to “Spreadsheet View” on page 118 for more information.

Frame Inspector View

Click on **Analysis** and select **Frame Inspector View** or click the icon to display the Frame Inspector View.



Length: 768 Bytes ☑ Hide Reserved Fields

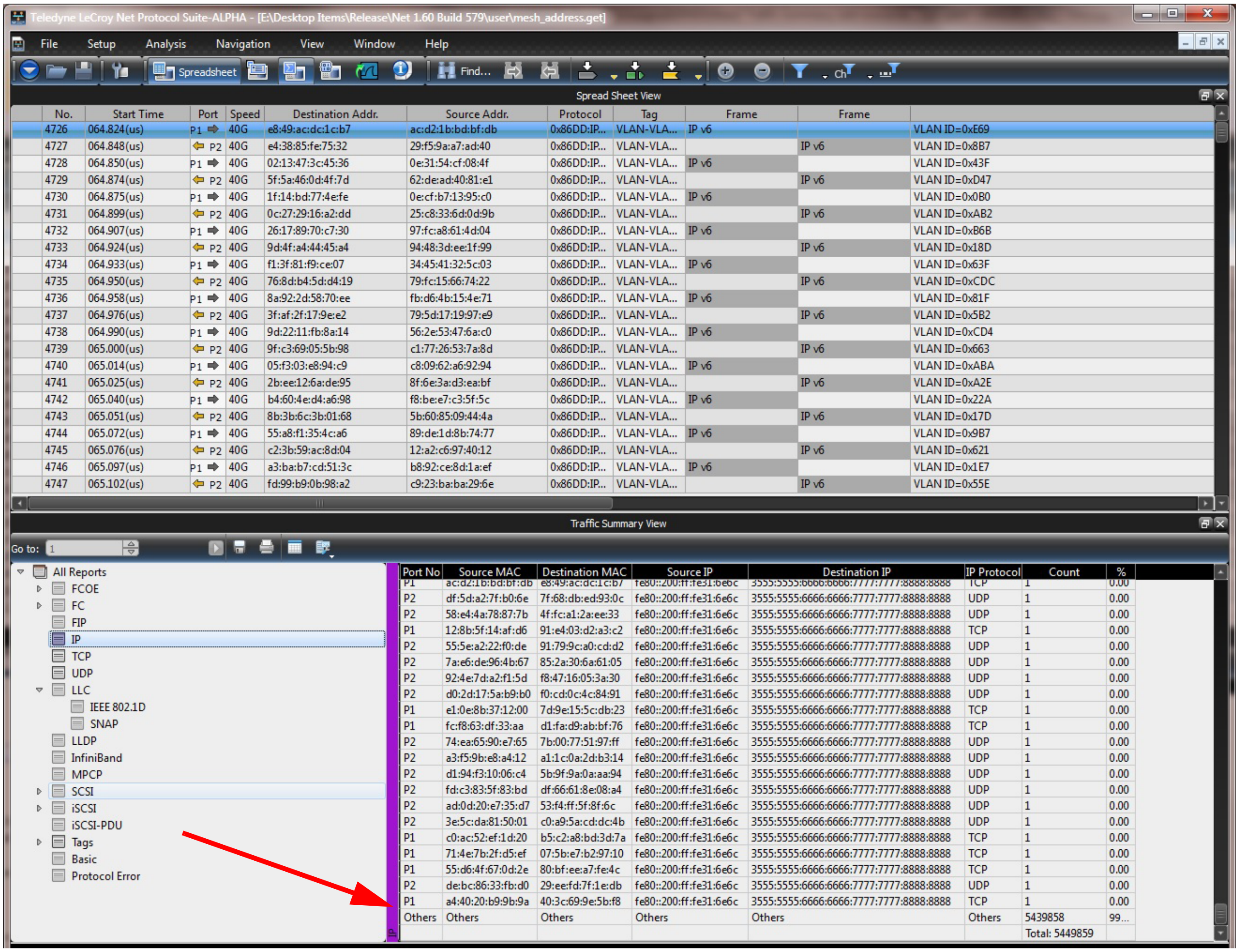
Field	Value
⊟ Ether Header	000E0CC6C1590017A43E348C8914
Destination Add.	000E0CC6C159
Source Add.	0017A43E348C
EtherType/Len	0x8914 : FIP
⊟ FIP Header	1000000300010007800002020017A43E348C0B050EFC001304000013040
Version	1
Protocol Code	0x0003 : FIP Keep Alive
SubCode	01
Descriptor List Length	0007
FP	1
SP	0
A	0
S	0
F	0
⊟ FIP Descriptor	02020017A43E348C
Type	0x02 : MAC address
Length	02
MAC address	0017A43E348C
⊟ FIP Descriptor	0B050EFC00130400001304000000000000000000
Type	0x0B : Vx_Port Identification

Figure 2.11: Frame Inspector View.

Frame Inspector View displays detail information about a frame highlighted in Spreadsheet view. Refer to “Frame Inspector View” on page 128 for more information.

Traffic Summary View

Click on **Analysis** and select **Traffic Summary View** or click the icon to display the Traffic Summary View.



No.	Start Time	Port	Speed	Destination Addr.	Source Addr.	Protocol	Tag	Frame	Frame	
4726	064.824(us)	P1 ➡	40G	e8:49:ac:dc:1c:b7	ac:d2:1b:bd:bf:db	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0xE69
4727	064.848(us)	⬅ P2	40G	e4:38:85:fe:75:32	29:f5:9a:a7:ad:40	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0x8B7
4728	064.850(us)	P1 ➡	40G	02:13:47:3c:45:36	0e:31:54:cf:08:4f	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0x43F
4729	064.874(us)	⬅ P2	40G	5f:5a:46:0d:4f:7d	62:de:ad:40:81:e1	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0xD47
4730	064.875(us)	P1 ➡	40G	1f:14:bd:77:4e:fe	0e:cf:b7:13:95:c0	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0x0B0
4731	064.899(us)	⬅ P2	40G	0c:27:29:16:a2:dd	25:c8:33:6d:0d:9b	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0xAB2
4732	064.907(us)	P1 ➡	40G	26:17:89:70:c7:30	97:fc:a8:61:4d:04	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0xB6B
4733	064.924(us)	⬅ P2	40G	9d:4f:a4:44:45:a4	94:48:3d:ee:1f:99	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0x18D
4734	064.933(us)	P1 ➡	40G	f1:3f:81:f9:ce:07	34:45:41:32:5c:03	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0x63F
4735	064.950(us)	⬅ P2	40G	76:8d:b4:5d:d4:19	79:fc:15:66:74:22	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0xCDC
4736	064.958(us)	P1 ➡	40G	8a:92:2d:58:70:ee	fb:d6:4b:15:4e:71	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0x81F
4737	064.976(us)	⬅ P2	40G	3f:af:2f:17:9e:e2	79:5d:17:19:97:e9	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0x5B2
4738	064.990(us)	P1 ➡	40G	9d:22:11:fb:8a:14	56:2e:53:47:6a:c0	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0xCD4
4739	065.000(us)	⬅ P2	40G	9f:c3:69:05:5b:98	c1:77:26:53:7a:8d	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0x663
4740	065.014(us)	P1 ➡	40G	05:f3:03:e8:94:c9	c8:09:62:a6:92:94	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0xABA
4741	065.025(us)	⬅ P2	40G	2b:ee:12:6a:de:95	8f:6e:3a:d3:ea:bf	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0xA2E
4742	065.040(us)	P1 ➡	40G	b4:60:4e:d4:a6:98	f8:be:e7:c3:5f:5c	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0x22A
4743	065.051(us)	⬅ P2	40G	8b:3b:6c:3b:01:68	5b:60:85:09:44:4a	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0x17D
4744	065.072(us)	P1 ➡	40G	55:a8:f1:35:4c:a6	89:de:1d:8b:74:77	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0x9B7
4745	065.076(us)	⬅ P2	40G	c2:3b:59:ac:8d:04	12:a2:c6:97:40:12	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0x621
4746	065.097(us)	P1 ➡	40G	a3:ba:b7:cd:51:3c	b8:92:ce:8d:1a:ef	0x86DD:IP...	VLAN-VLA...	IP v6		VLAN ID=0x1E7
4747	065.102(us)	⬅ P2	40G	fd:99:b9:0b:98:a2	c9:23:ba:ba:29:6e	0x86DD:IP...	VLAN-VLA...		IP v6	VLAN ID=0x55E

Port No	Source MAC	Destination MAC	Source IP	Destination IP	IP Protocol	Count	%
P1	ac:d2:1b:bd:bf:db	e8:49:ac:dc:1c:b7	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	TCP	1	0.00
P2	df:5d:a2:7f:b0:6e	7f:68:db:ed:93:0c	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	58:e4:4a:78:87:7b	4f:fc:a1:2a:ee:33	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P1	12:8b:5f:14:af:d6	91:e4:03:d2:a3:c2	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	TCP	1	0.00
P2	55:5e:a2:22:f0:de	91:79:9c:a0:cd:d2	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	7a:e6:de:96:4b:67	85:2a:30:6a:61:05	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	92:4e:7d:a2:f1:5d	f8:47:16:05:3a:30	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	d0:2d:17:5a:b9:b0	f0:cd:0c:4c:84:91	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P1	e1:0e:8b:37:12:00	7d:9e:15:5c:db:23	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	TCP	1	0.00
P1	fc:f8:63:df:33:aa	d1:fa:d9:ab:bf:76	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	TCP	1	0.00
P2	74:ea:65:90:e7:65	7b:00:77:51:97:ff	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	a3:f5:9b:e8:a4:12	a1:1c:0a:2d:b3:14	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	d1:94:f3:10:06:c4	5b:9f:9a:0a:aa:94	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	fd:c3:83:5f:83:bd	df:66:61:8e:08:a4	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	ad:0d:20:e7:35:d7	53:f4:ff:5f:8f:6c	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P2	3e:5c:da:81:50:01	c0:a9:5a:cd:dc:4b	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P1	c0:ac:52:ef:1d:20	b5:c2:a8:bd:3d:7a	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	TCP	1	0.00
P1	71:4e:7b:2f:d5:ef	07:5b:e7:b2:97:10	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	TCP	1	0.00
P1	55:d6:4f:67:0d:2e	80:bf:ee:a7:fe:4c	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	TCP	1	0.00
P2	de:bc:86:33:fb:d0	29:ee:fd:7f:1e:db	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	UDP	1	0.00
P1	a4:40:20:b9:9b:9a	40:3c:69:9e:5b:f8	fe80::200:ff:fe31:6e6c	3555:5555:6666:6666:7777:7777:8888:8888	TCP	1	0.00
Others	Others	Others	Others	Others	Others	5439858	99...
						Total: 5449859	

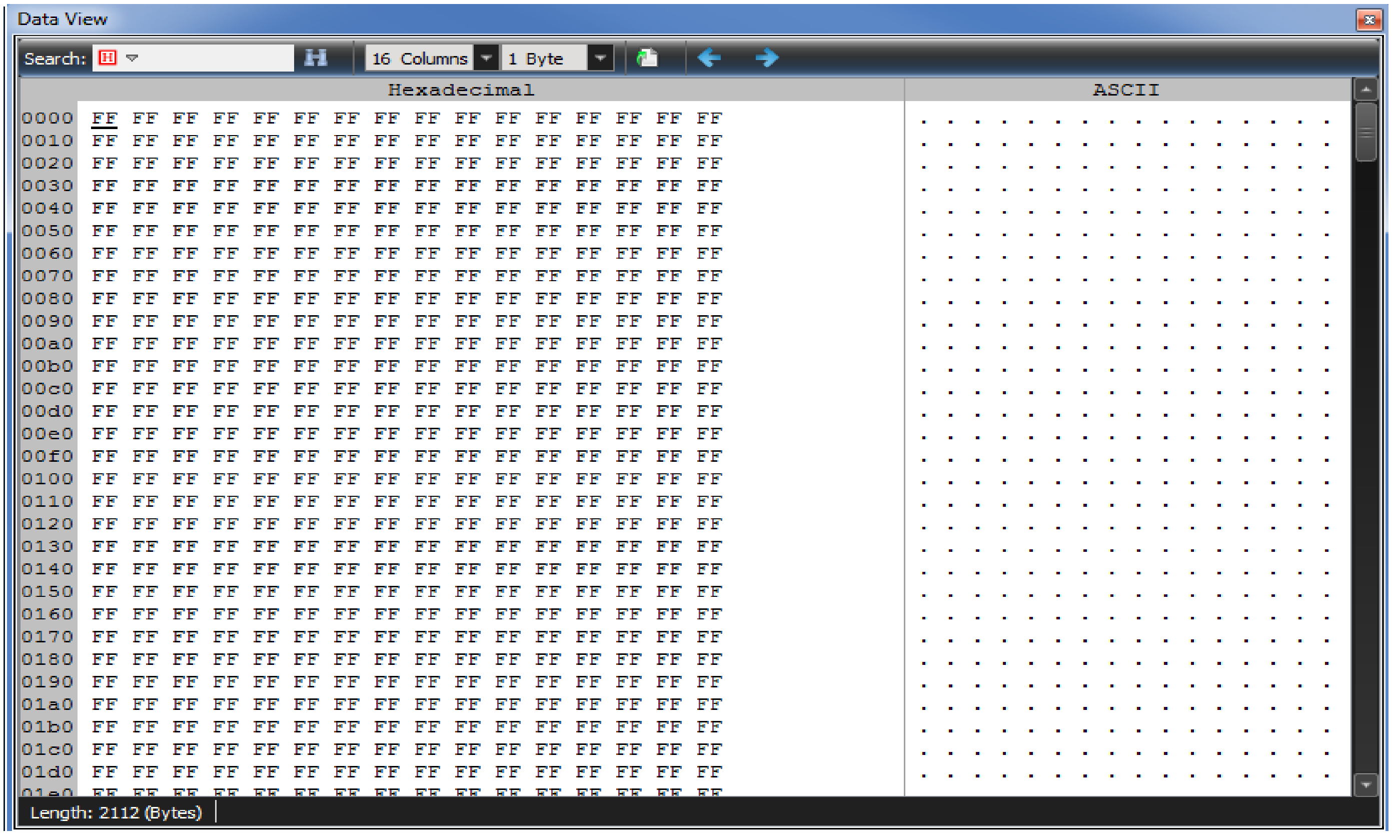
Figure 2.12: Traffic Summary View.

The Traffic Summary View for each captured signal can be viewed. This Summary View displays the statistics of commands, the type of command and the total count. For each command it displays the percent of the total count.

The software collects up to 10,000 unique pairs for the reports. Anything beyond that is grouped into the "Others" category as shown in Figure 2.12.

Data View

Click on **Analysis** and select **Data View** or click the icon to display the Data View (see Figure 2.13 on page 44).



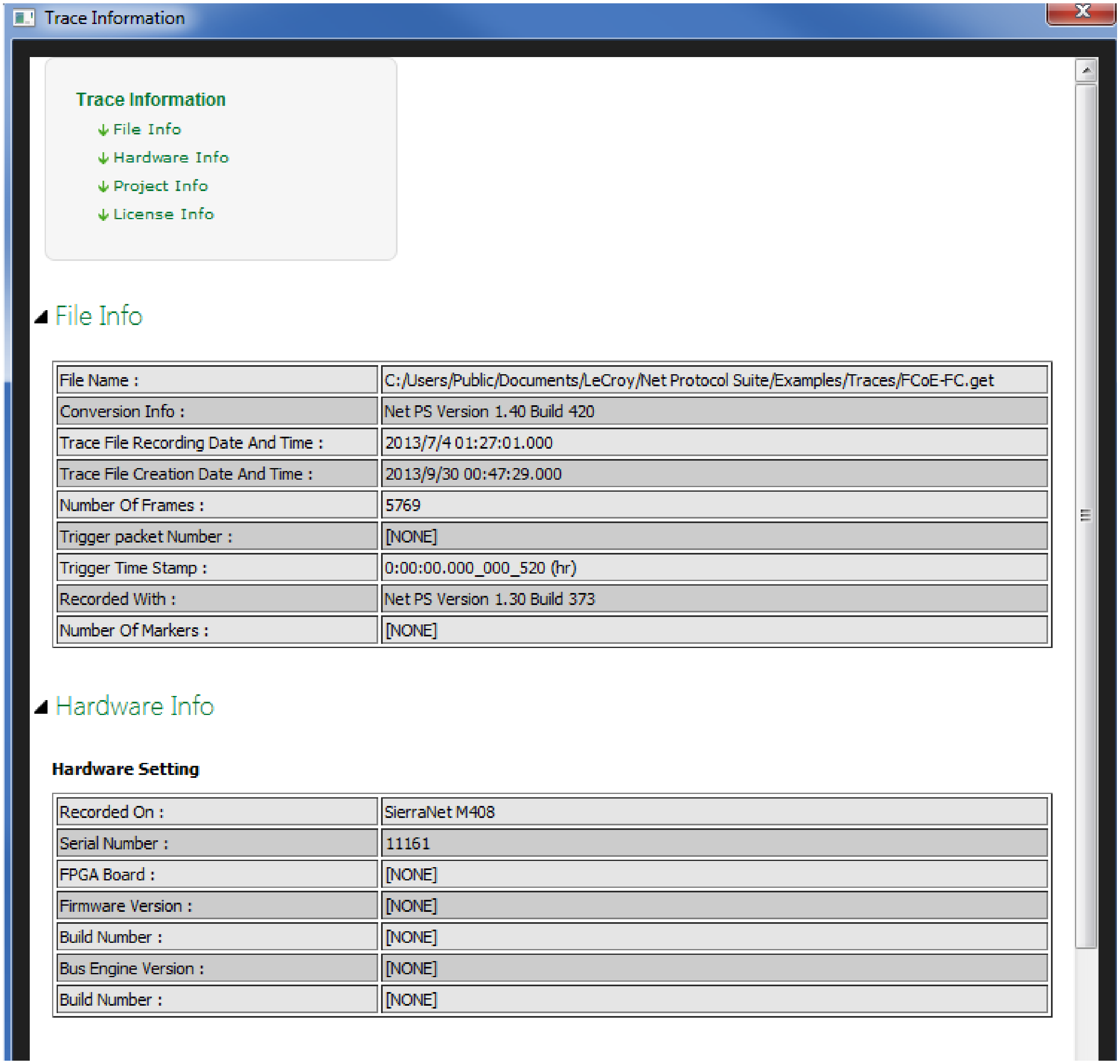
```
                  Hexadecimal                                        ASCII
0000 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0010 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0020 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0030 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0040 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0050 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0060 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0070 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0080 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0090 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
00a0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
00b0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
00c0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
00d0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
00e0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
00f0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0100 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0110 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0120 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0130 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0140 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0150 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0160 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0170 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0180 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
0190 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
01a0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
01b0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
01c0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
01d0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    . . . . . . . . . . . . . . . .
01e0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
Length: 2112 (Bytes)
```

Figure 2.13: Data View.

The Data View displays information in Hexadecimal and ASCII format. Refer to “Data View” on page 134 for more information.

Trace Information

Click on **Analysis** and select **Trace Information** or click the ℹ icon to display the trace Information dialog (see Figure 2.14 on page 45 and Figure 2.15 on page 46). You can click on the hyperlinks: **File info**, **Hardware info**, **Project info** or **License info** to navigate to that section. Click **Open Trace Project** to open the project in which the trace was captured.



Trace Information

- File Info
- Hardware Info
- Project Info
- License Info

File Info

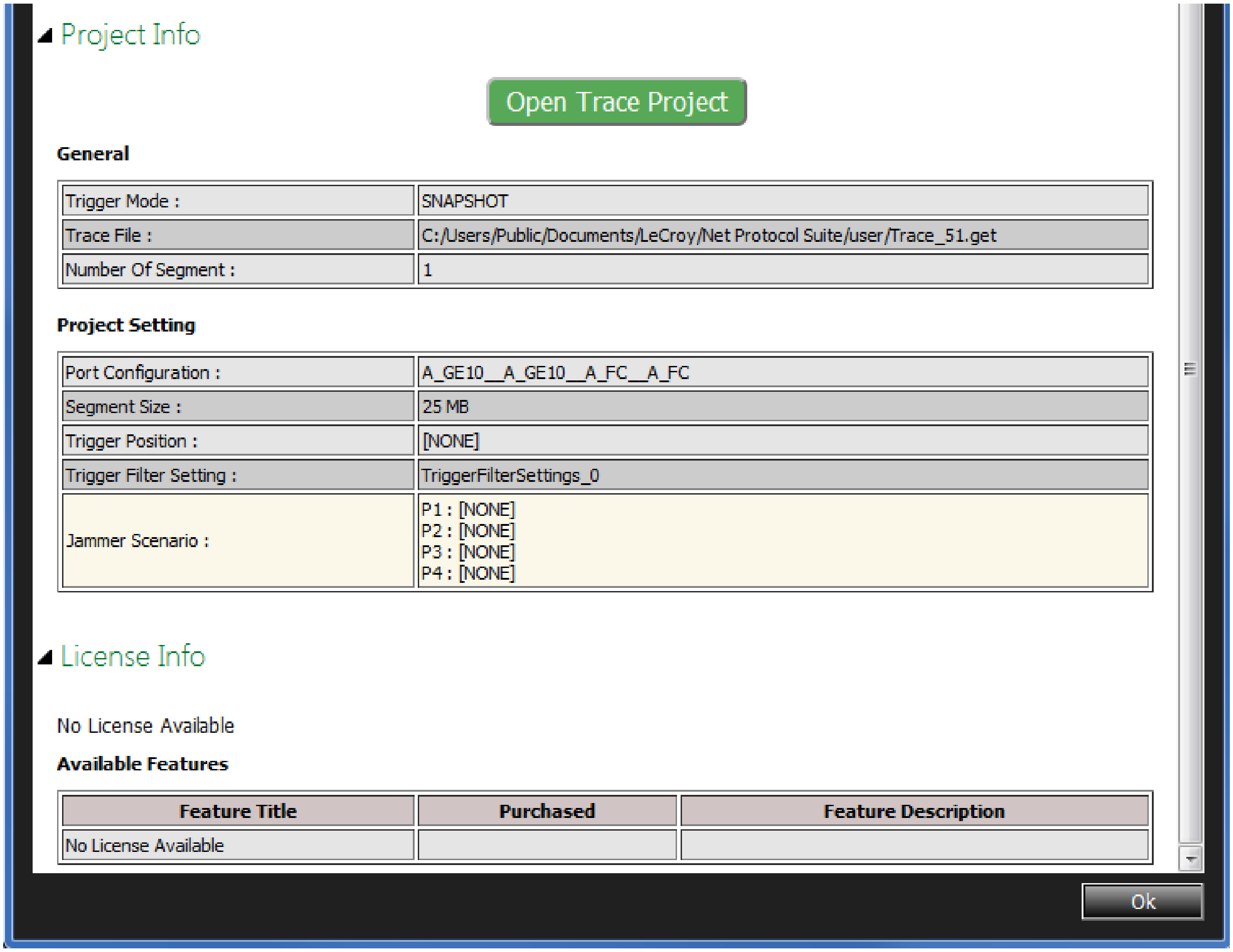
File Name :	C:/Users/Public/Documents/LeCroy/Net Protocol Suite/Examples/Traces/FCoE-FC.get
Conversion Info :	Net PS Version 1.40 Build 420
Trace File Recording Date And Time :	2013/7/4 01:27:01.000
Trace File Creation Date And Time :	2013/9/30 00:47:29.000
Number Of Frames :	5769
Trigger packet Number :	[NONE]
Trigger Time Stamp :	0:00:00.000_000_520 (hr)
Recorded With :	Net PS Version 1.30 Build 373
Number Of Markers :	[NONE]

Hardware Info

Hardware Setting

Recorded On :	SierraNet M408
Serial Number :	11161
FPGA Board :	[NONE]
Firmware Version :	[NONE]
Build Number :	[NONE]
Bus Engine Version :	[NONE]
Build Number :	[NONE]

Figure 2.14: Trace Information Dialog 1.



General

Trigger Mode :	SNAPSHOT
Trace File :	C:/Users/Public/Documents/LeCroy/Net Protocol Suite/user/Trace_51.get
Number Of Segment :	1

Project Setting

Port Configuration :	A_GE10__A_GE10__A_FC__A_FC
Segment Size :	25 MB
Trigger Position :	[NONE]
Trigger Filter Setting :	TriggerFilterSettings_0
Jammer Scenario :	P1 : [NONE] P2 : [NONE] P3 : [NONE] P4 : [NONE]

No License Available

Available Features

Feature Title	Purchased	Feature Description
No License Available		

Figure 2.15: Trace Information Dialog 2.

2.5.4 Navigation

The Navigation menu option enables the user to navigate the application (see Figure 2.16 on page 47). You can go to the trigger, marker or where the cursor is located. Markers can also be added and removed. Find menu options are available as shown in the screen capture below.

Note: The menu options listed in the Navigation menu can also be selected when you right-click anywhere on the screen, see “Markers” on page 127.

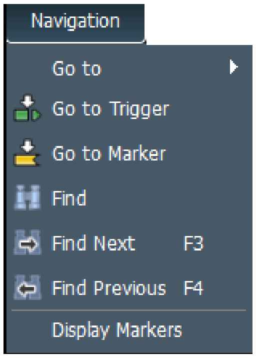


Figure 2.16: Navigation Menu Option.

The Navigation menu currently has the following options (see Figure 2.16 on page 47).

- **Go To** menu options allows location of cursors or specific packets: Timestamp, X Position, Y Position, Event, Begin, and End. Refer to Figure 2.17.

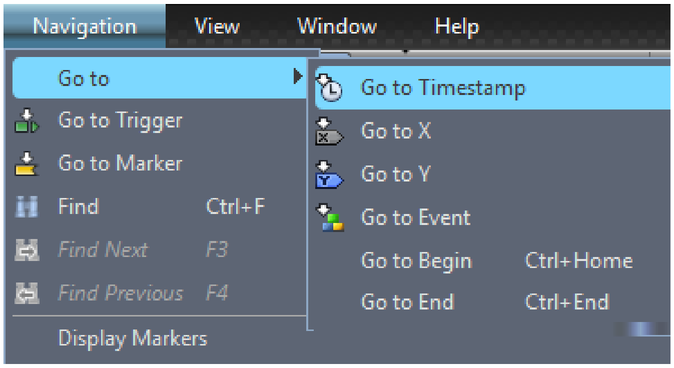


Figure 2.17: Navigation Go to Menu Option.

- Go to Trigger- Allows you to go to the trigger point in the trace.
- Go to Marker- Allows you to go to specific Marker (see “Markers” on page 127).
- Find - Allows you to examine any data capture file to quickly locate the packet or data pattern (see “Find” on page 144).
- Find Next - Gives you the option to search for the next instance (see “Find” on page 144).
- Find Previous - Gives you the option to search for the previous instance (see “Find” on page 144).
- Display Markers - Displays the list of markers (see “Markers” on page 127).

2.5.5 View

The View menu has the following options:

- Zoom in- Allows you to zoom in the view.
- Zoom out- Allows you to zoom out the view.
- Hide/Show -Displays the Filter dialog box enabling you to configure filters applied to the trace view.
- Hide/Show non-Frames - Shows/Hides the Idles in the trace view.
- Toolbars-Allows you to customize the toolbar display (see Figure 2.18 on page 48).
- Menu Bar-Selecting and deselecting this option toggles between showing and hiding the menu bar. Press the Alt + Windows keys to do the same.

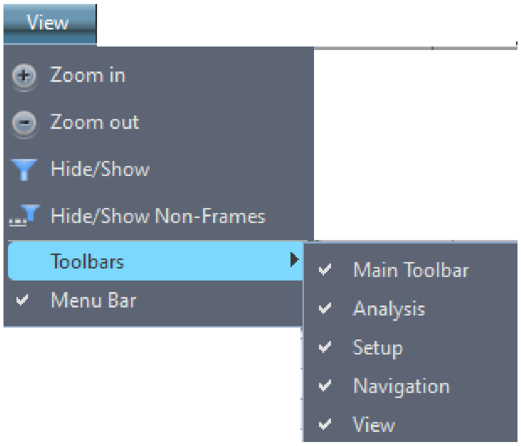


Figure 2.18: View Menu Option.

2.5.6 Window

Window - Allows you to configure your display. It has the following options:

- Window Cascade (see “Switching Views” on page 117).
- Window Tile (see “Switching Views” on page 117).
- Close All Traces - closes all open traces

2.5.7 Help

The Help menu (see Figure 2.19 on page 49) currently has the following options:

Tell Teledyne LeCroy

Report a problem to Teledyne LeCroy Support via e-mail by selecting **Help>Tell Teledyne LeCroy** from the application toolbar. This requires that an e-mail client be installed and configured on the host machine.

Help Topics

Displays the User Manual.

License Information

Displays the License information with the licences that are purchased and their features (see “License Information” on page 160).

Check for Updates

Checks to see if there are any updates available for download “Check for Updates” on page 161.

Shortcut List

Displays a list of keyboard shortcuts (see “Shortcut List” on page 161).

About

Displays the current Net Protocol Suite information, see “About” on page 162.

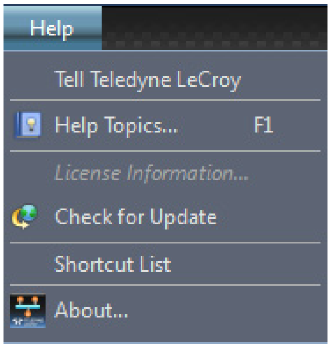


Figure 2.19: Help Menu Option.

2.6 Analyzer Settings

The Teledyne LeCroy Ethernet Protocol Suite Analyzer Settings panel in the application has six functional sections as shown below. The application is designed such that the user starts from the left pane and moves to the right pane to connect to a device and record a capture as listed below.

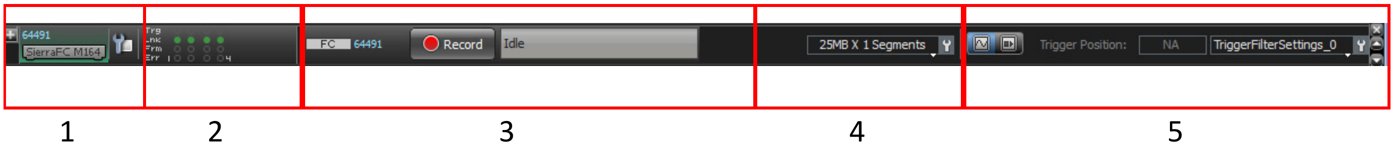


Figure 2.20: Analyzer Settings Panel.

1. Device Pane: Enables adding and assigning a device.
2. Port Status Pane: View the port status.
3. Session Control Pane: Starts and stops recording.
4. Recording Settings Pane: Manage the recording settings such as Number of Segments and Segment Size.
5. Trigger/Filter Settings Pane: Enables Trigger Filter settings.

2.6.1 Device Pane

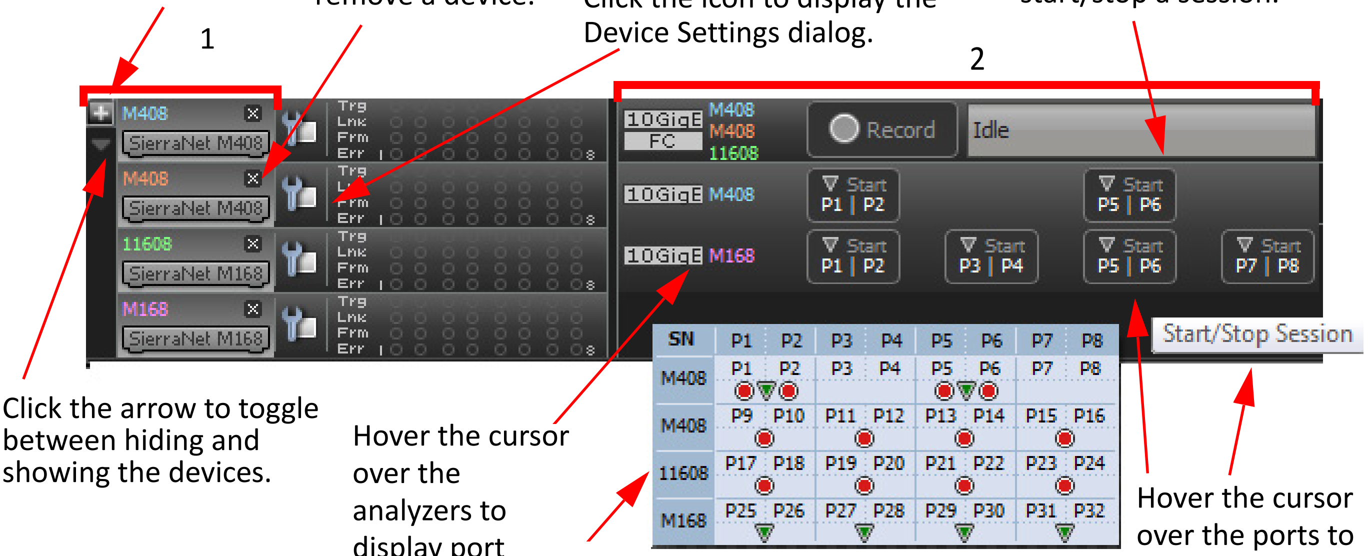
The Device pane allows you to add or remove a device in the chain of attached devices and assign each device to a different project (see Figure 2.21 on page 50). You must first add a device before activating it by clicking **Setup > Device Management** to select a device drag-and-drop it onto a device in the Project Device Pane. You can have multiple projects assigned to different devices. A single project will automatically connect to an active device. Right-click on a device and select **Activate** to start the device. Click The X icon to disconnect the device.

Click the + sign to add a device.

Click the x sign to remove a device.

Click the icon to display the Device Settings dialog.

Click any of the ports to start/stop a session.



SN	P1	P2	P3	P4	P5	P6	P7	P8
M408	P1	P2	P3	P4	P5	P6	P7	P8
M408	P9	P10	P11	P12	P13	P14	P15	P16
11608	P17	P18	P19	P20	P21	P22	P23	P24
M168	P25	P26	P27	P28	P29	P30	P31	P32

Click the arrow to toggle between hiding and showing the devices.

Hover the cursor over the analyzers to display port configurations.

Hover the cursor over the ports to display tooltip.

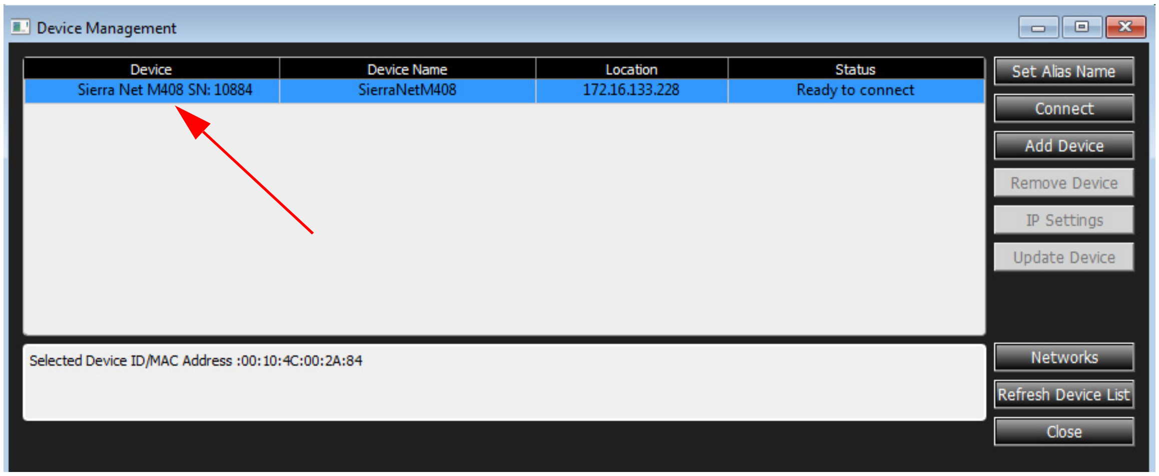
Figure 2.21: Device Pane Displaying Multiple Devices.

- ❑ Presents a physical representation of the analyzers.
- ❑ Presents a logical representation of the analyzers.

Perform the following steps to add a device.

1. Click **Setup > Device Management.**

   The **Device Management** dialog displays.



Device	Device Name	Location	Status
Sierra Net M408 SN: 10884	SierraNetM408	172.16.133.228	Ready to connect

Selected Device ID/MAC Address :00:10:4C:00:2A:84

2. Click on the selected Device (Sierra Net M408 SN: 10884) and select the **Connect** button.

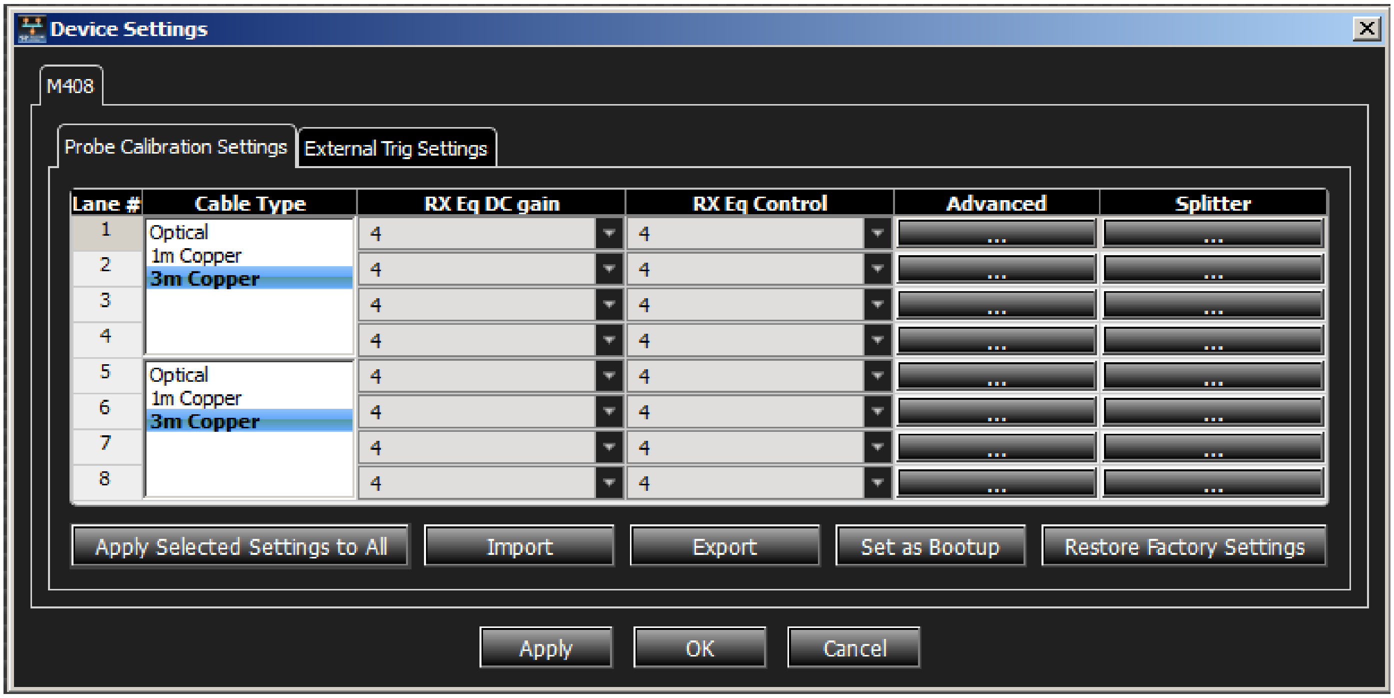
Device Settings

The Device Settings dialog allows you to configure Probe Calibration and the External Trigger settings for each device. See “Probe Calibration” on page 51 and “External Trigger” on page 58 for more information.

2.6.2 Probe Calibration

In the Device Settings dialog, select the Probe Calibration Settings tab. Depending on the project's protocol configuration, the Device Settings tab appears slightly different. These settings are meant for advanced users to tune the performance of the Analyzer's receiver ports, the Jammer's receiver and transmitter ports, and the Analyzer's DUT link pass-through path. In most cases, the default settings will perform well and should be used as-is.

40 GigE Configurations



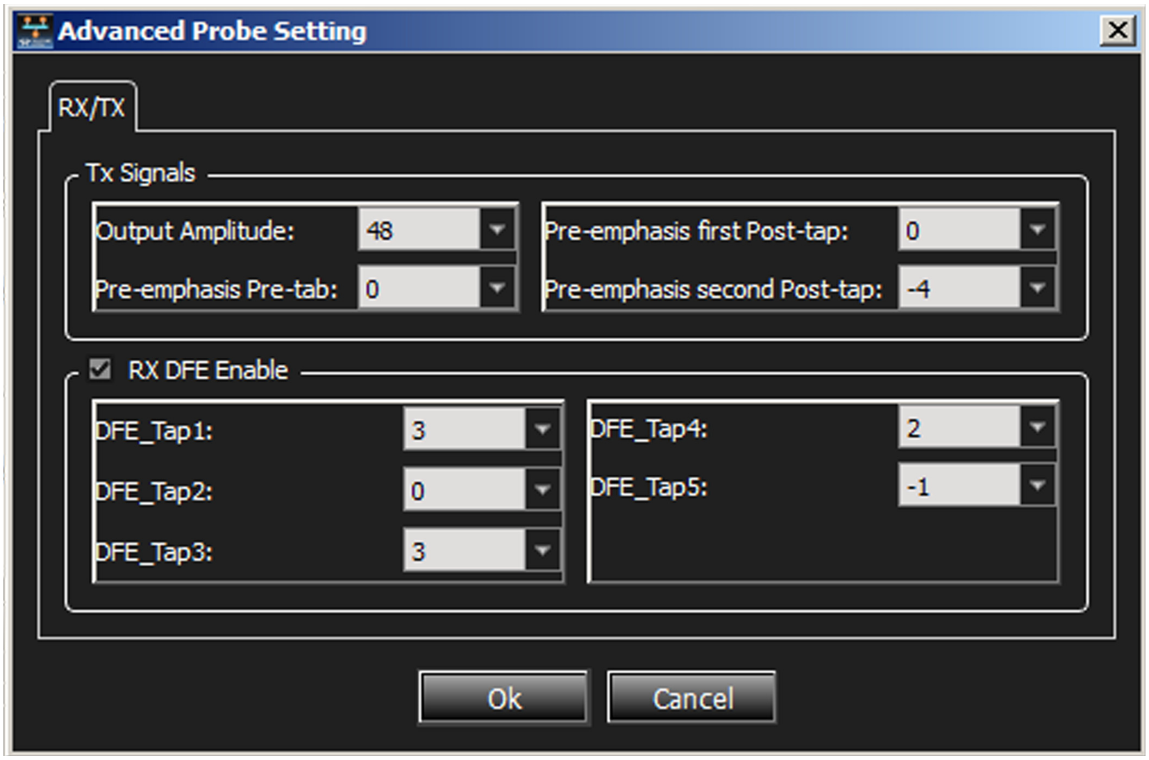
Lane #	Cable Type	RX Eq DC gain	RX Eq Control	Advanced	Splitter
1	Optical 1m Copper 3m Copper	4	4	...	...
2		4	4	...	...
3		4	4	...	...
4		4	4	...	...
5	Optical 1m Copper 3m Copper	4	4	...	...
6		4	4	...	...
7		4	4	...	...
8		4	4	...	...

Figure 2.22: Device Settings dialog for 40 GigE device.

You can manually calibrate the probe settings. Set the parameters for the following:

- Cable Type: Select Optical, 1m Copper or 3m Copper.
- RX Eq DC gain: Select a value from the drop-down list.
- RX Eq Control: Select a value from the drop-down list.
- Advanced: Selecting **Advanced** displays the Advanced Probe Setting dialog. (See Figure 2.23.) Enter the desired values for each of the parameters.
- Splitter: Selecting **Splitter** displays the Splitter Settings dialog. (See Figure 2.24 on page 52.)
- Apply Selected Settings to All: Applies the settings selected in the currently selected port to all ports in the list.

- Import: Loads calibration settings from *.csv file.
- Export: Creates a new *.csv file.
- Set as Bootup: Loads these settings into memory; rebooting will automatically load these values.
- Restore Factory Settings: Restores factory settings.



Advanced Probe Setting

RX/TX

Tx Signals

Output Amplitude: 48

Pre-emphasis Pre-tab: 0

Pre-emphasis first Post-tap: 0

Pre-emphasis second Post-tap: -4

☑ RX DFE Enable

DFE_Tap1: 3

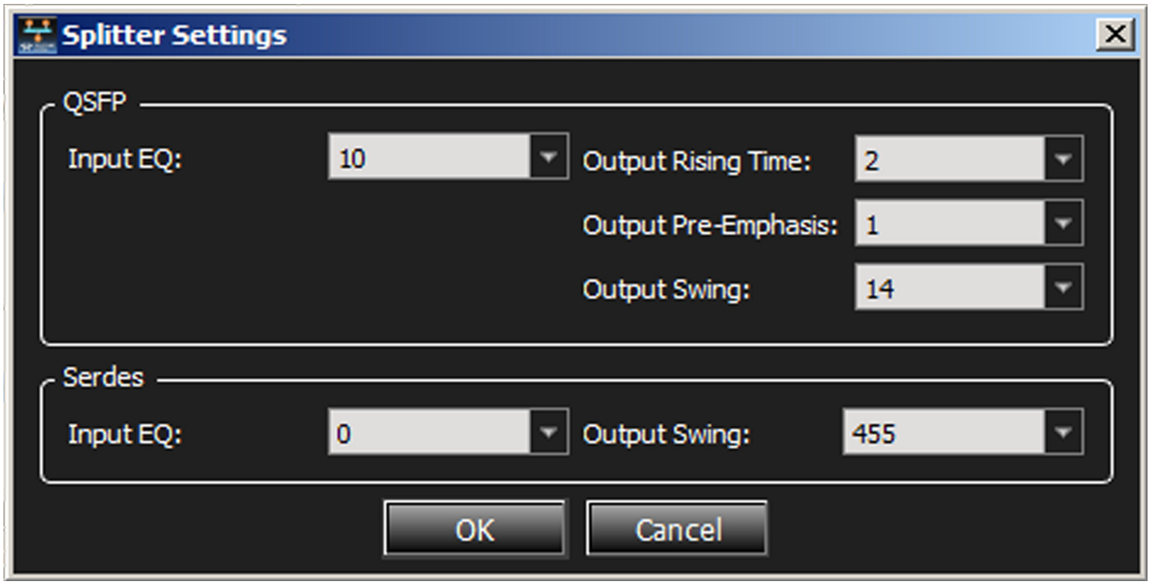
DFE_Tap2: 0

DFE_Tap3: 3

DFE_Tap4: 2

DFE_Tap5: -1

Figure 2.23: Advanced Probe Setting dialog for 40 GigE device.



Splitter Settings

QSFP

Input EQ: 10

Output Rising Time: 2

Output Pre-Emphasis: 1

Output Swing: 14

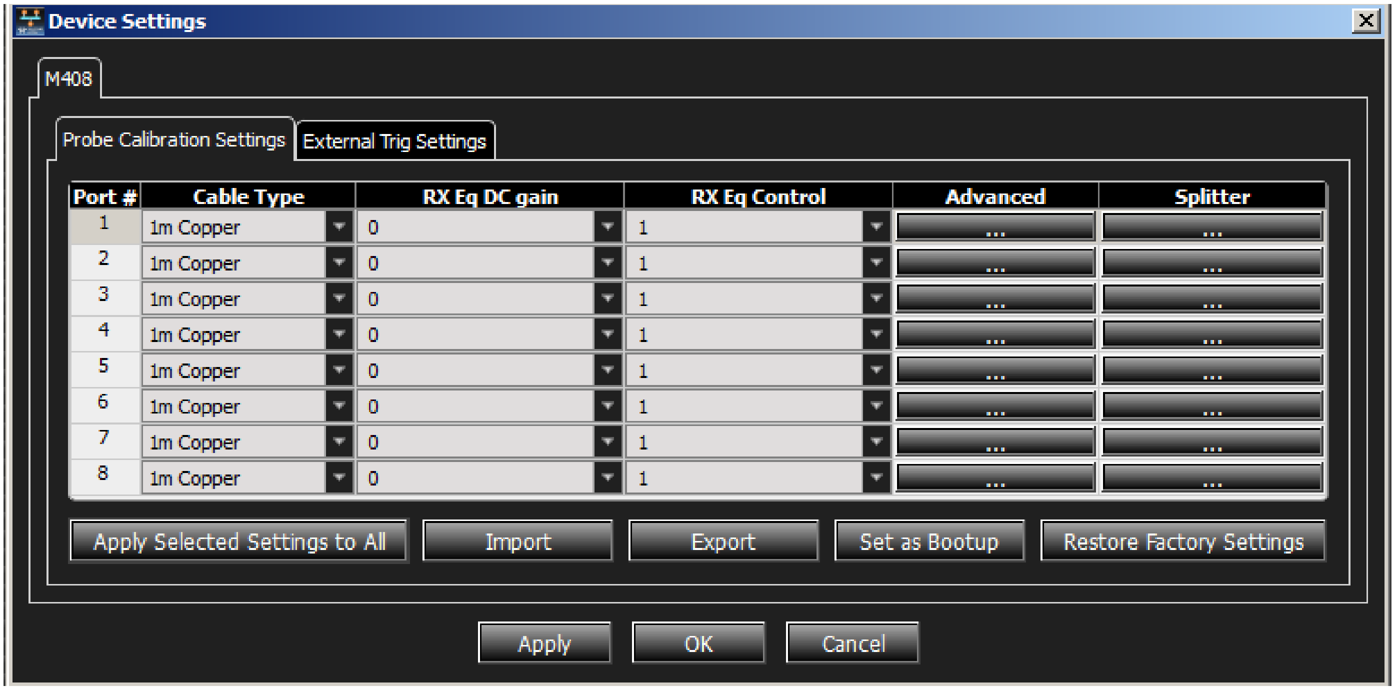
Serdes

Input EQ: 0

Output Swing: 455

Figure 2.24: Splitter Settings dialog for 40 GigE device.

10 GigE Configurations



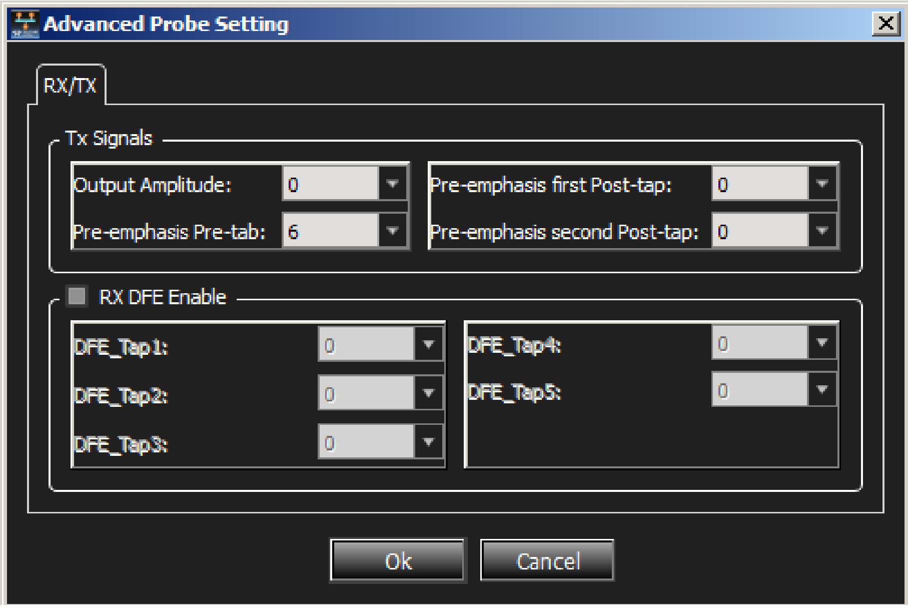
Port #	Cable Type	RX Eq DC gain	RX Eq Control	Advanced	Splitter
1	1m Copper	0	1	...	...
2	1m Copper	0	1	...	...
3	1m Copper	0	1	...	...
4	1m Copper	0	1	...	...
5	1m Copper	0	1	...	...
6	1m Copper	0	1	...	...
7	1m Copper	0	1	...	...
8	1m Copper	0	1	...	...

Figure 2.25: Device Settings dialog for 10 GigE device.

You can manually calibrate the probe settings.

Set the parameters for the following:

- Cable Type: Select Optical, 1m Copper or 3m Copper.
- RX Eq DC gain: Select a value from the drop-down list.
- RX Eq Control: Select a value from the drop-down list.
- Advanced: Selecting **Advanced** displays the Advanced Probe Setting dialog. (See Figure 2.26.) Enter the desired values for each of the parameters.
- Splitter: Selecting **Splitter** displays the Splitter Settings dialog. (See Figure 2.27 on page 54.)
- Apply Selected Settings to All: Applies the settings selected in the currently selected port to all ports in the list.
- Import: Loads calibration settings from *.csv file.
- Export: Creates a new *.csv file.
- Set as Bootup: Loads these settings into memory; rebooting will automatically load these values.
- Restore Factory Settings: Restores factory settings.



Tx Signals

Output Amplitude: 0

Pre-emphasis Pre-tab: 6

Pre-emphasis first Post-tap: 0

Pre-emphasis second Post-tap: 0

□ RX DFE Enable

DFE_Tap1: 0

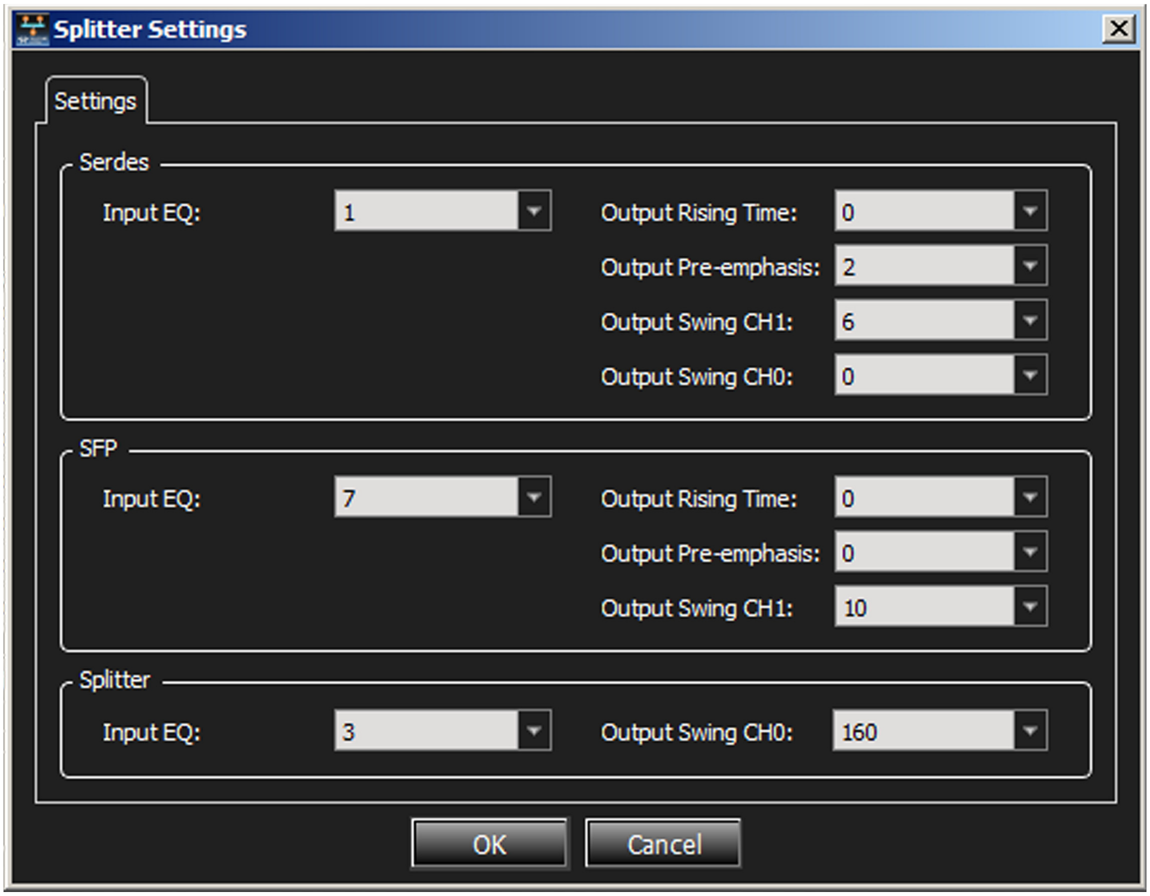
DFE_Tap2: 0

DFE_Tap3: 0

DFE_Tap4: 0

DFE_Tap5: 0

Figure 2.26: Advanced Probe Setting dialog for 10 GigE device.



Serdes

Input EQ: 1

Output Rising Time: 0

Output Pre-emphasis: 2

Output Swing CH1: 6

Output Swing CH0: 0

SFP

Input EQ: 7

Output Rising Time: 0

Output Pre-emphasis: 0

Output Swing CH1: 10

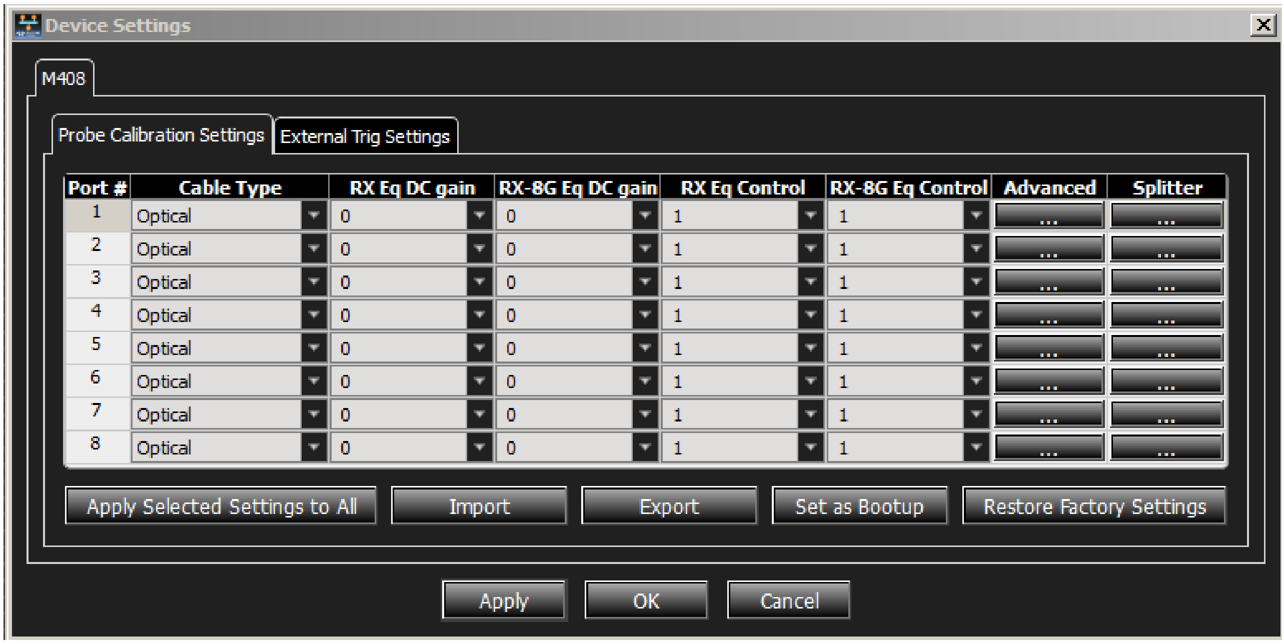
Splitter

Input EQ: 3

Output Swing CH0: 160

Figure 2.27: Splitter Settings dialog for 10 GigE device.

FC Configurations

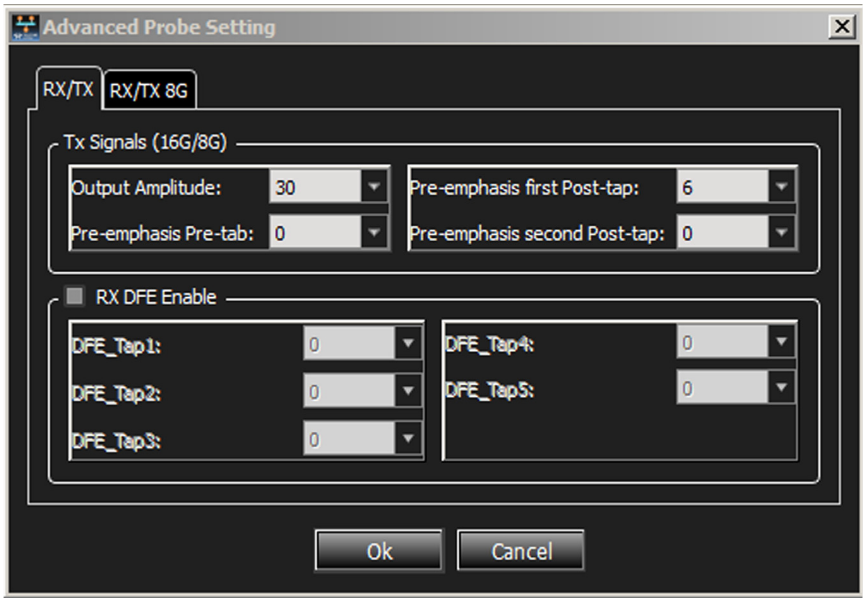


Port #	Cable Type	RX Eq DC gain	RX-8G Eq DC gain	RX Eq Control	RX-8G Eq Control	Advanced	Splitter
1	Optical	0	0	1	1	...	...
2	Optical	0	0	1	1	...	...
3	Optical	0	0	1	1	...	...
4	Optical	0	0	1	1	...	...
5	Optical	0	0	1	1	...	...
6	Optical	0	0	1	1	...	...
7	Optical	0	0	1	1	...	...
8	Optical	0	0	1	1	...	...

Figure 2.28: Device Settings dialog for FC devices.

You can manually calibrate the probe settings. Set the parameters for the following:

- Cable Type
- RX Eq DC gain: Select value from the drop-down list.
- RX-8G Eq DC gain: Select value from the drop-down list.
- RX Eq Control: Select value from the drop-down list.
- RX-8G Eq Control: Select value from the drop-down list.
- Advanced: Selecting **Advanced** displays the Advanced Probe Setting dialog with the RX/TX tab selected. (See Figure 2.29.) Enter the desired values for each of the parameters. Select the RX/TX 8G tab (see Figure 2.30 on page 56) and enter the desired values for each of the parameters.
- Splitter: Selecting **Splitter** displays the Splitter Settings dialog. (See Figure 2.31 on page 57.) Enter the desired values for each of the parameters. Select the 8G tab (see Figure 2.32 on page 57) and enter the desired values for each of the parameters.
- Apply Selected Settings to All: Applies the settings selected in the currently selected port to all ports in the list.
- Import: Loads calibration settings from *.csv file.
- Export: Creates a new *.csv file.
- Set as Bootup: Loads these settings into memory; rebooting will automatically load these values.
- Restore Factory Settings: Restores factory settings.



Tx Signals (16G/8G)

Output Amplitude: 30

Pre-emphasis Pre-tab: 0

Pre-emphasis first Post-tap: 6

Pre-emphasis second Post-tap: 0

□ RX DFE Enable

DFE_Tap1: 0

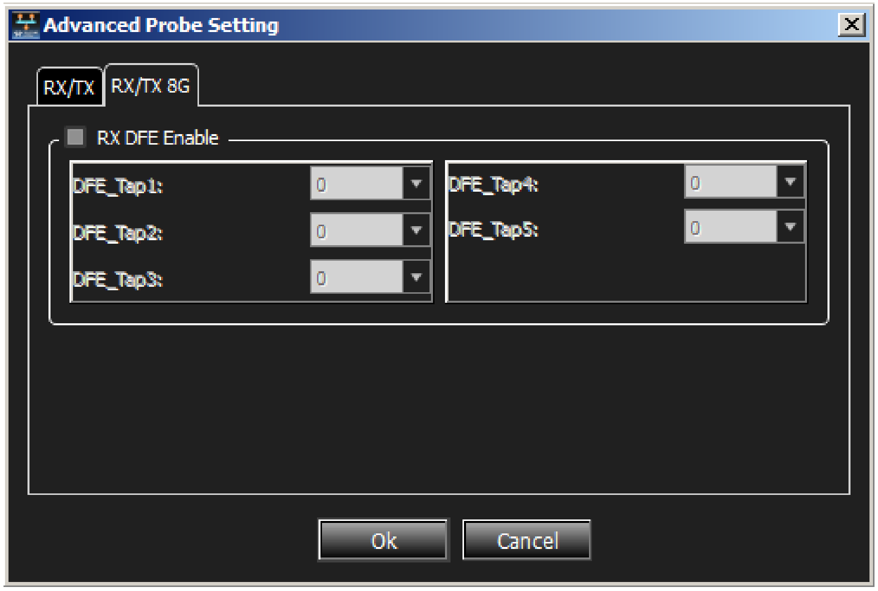
DFE_Tap2: 0

DFE_Tap3: 0

DFE_Tap4: 0

DFE_Tap5: 0

Figure 2.29: Advanced Probe Setting dialog for FC device - RX/TX tab.



□ RX DFE Enable

DFE_Tap1: 0

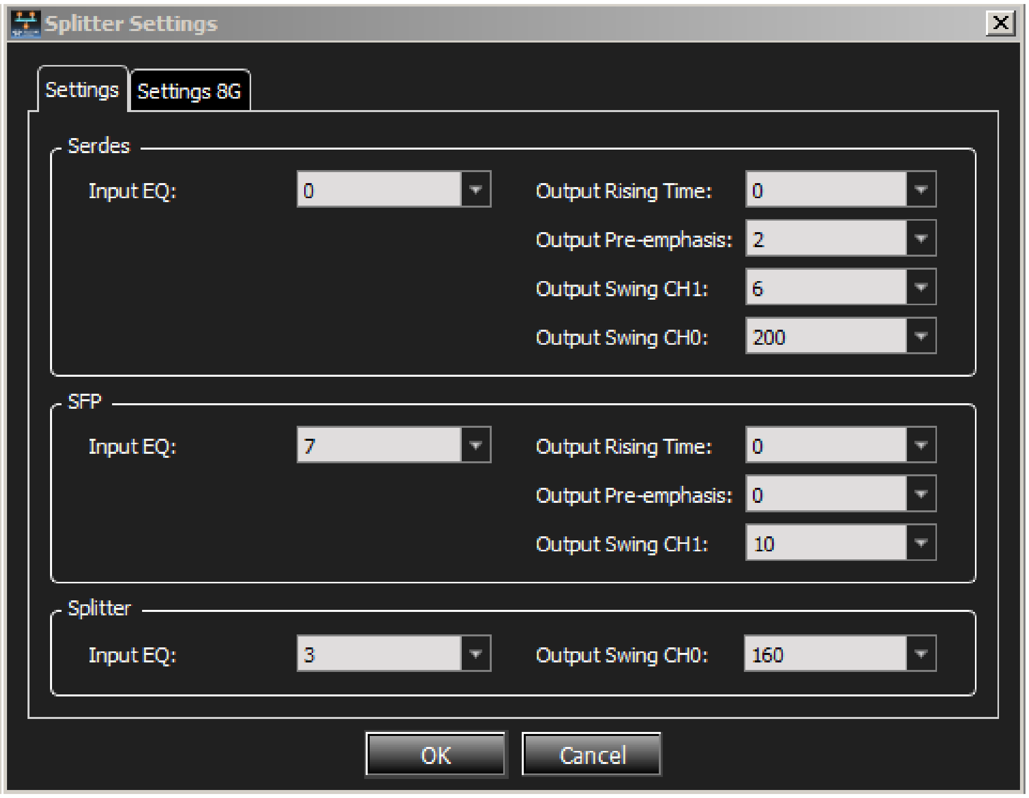
DFE_Tap2: 0

DFE_Tap3: 0

DFE_Tap4: 0

DFE_Tap5: 0

Figure 2.30: Advanced Probe Setting dialog for FC device - RX/TX 8G tab.



Serdes

Input EQ: 0

Output Rising Time: 0

Output Pre-emphasis: 2

Output Swing CH1: 6

Output Swing CH0: 200

SFP

Input EQ: 7

Output Rising Time: 0

Output Pre-emphasis: 0

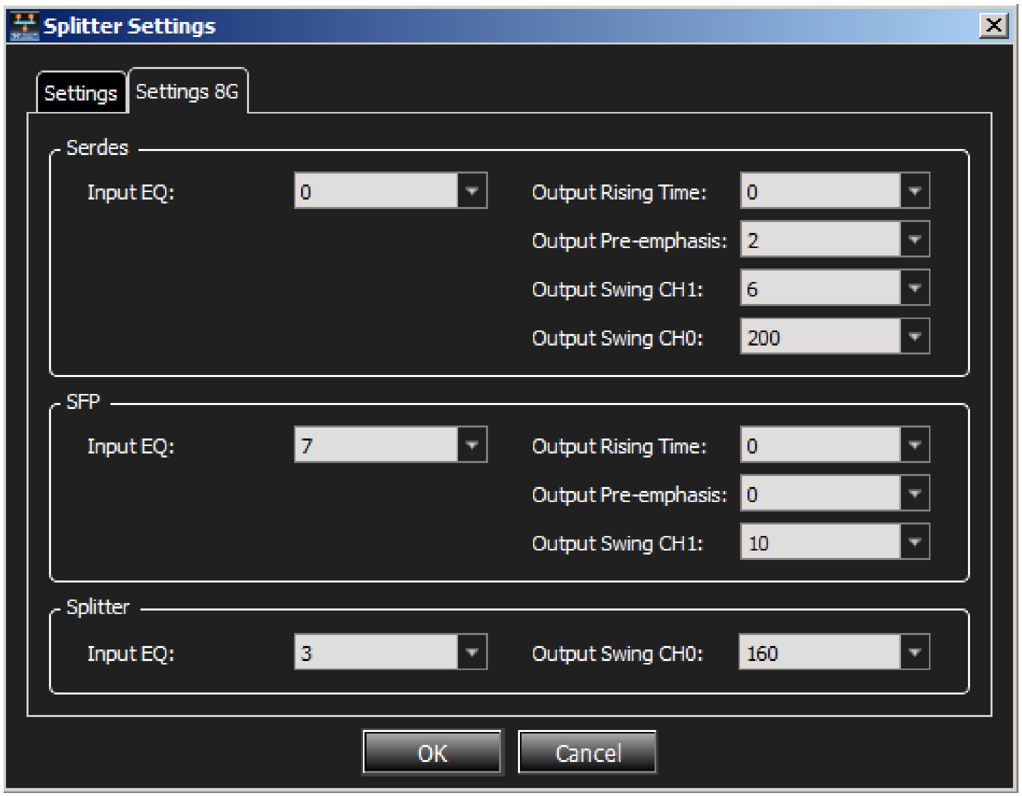
Output Swing CH1: 10

Splitter

Input EQ: 3

Output Swing CH0: 160

Figure 2.31: Splitter Settings dialog for FC device.



Serdes

Input EQ: 0

Output Rising Time: 0

Output Pre-emphasis: 2

Output Swing CH1: 6

Output Swing CH0: 200

SFP

Input EQ: 7

Output Rising Time: 0

Output Pre-emphasis: 0

Output Swing CH1: 10

Splitter

Input EQ: 3

Output Swing CH0: 160

Figure 2.32: Splitter Settings dialog for FC device - 8G tab.

External Trigger

Note: This dialog applies to all configurations.

In the Device Settings dialog, selectelect the External Trig Settings tab which shows the External Trig Out Setting and External Trig In Setting as Active, Active Low, or Toggle.

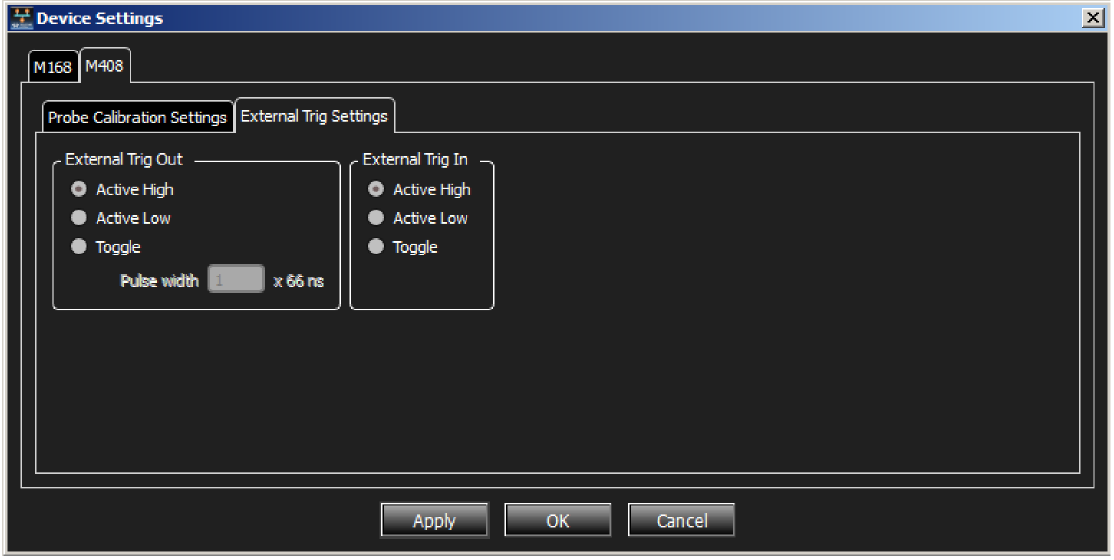


Figure 2.33: External Trigger Settings dialog.

External Trig Out Setting
The Analyzer can send a Low or High external signal any time a trigger occurs.

Select the External Trig Out Setting: High Active, Low Active, or Toggle from High to Low or Low to High once (3.3 V output).

Enter the External TrigOut pulse width.

External Trig In Setting
An external Low or High input signal can cause triggering.

Select the External Trig In Setting: High Active, Low Active, or Toggle from High to Low or Low to High once (3.3 V output).

The nominal External Trigger voltage is 0.818 volts. Trigger In can work with 1 volt to 5 volts input voltage.

2.6.3 Port Status Pane

The Port Status pane (see Figure 2.34 on page 59) displays the status of the link on each port (Trigger, Link, Frame and Error). Right-click the pane and select the **Reset** button to reset the status.

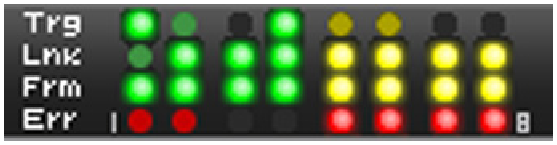
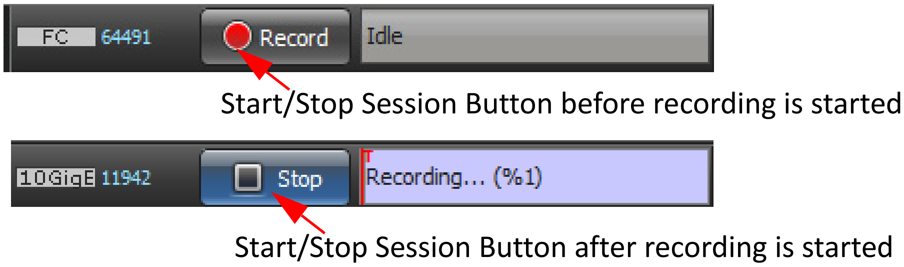


Figure 2.34: Port Status Pane.

2.6.4 Session Control Pane

Use the Session Control pane (see Figure 2.35 on page 59) to run and stop a capture. You can also set the idle.



Start/Stop Session Button before recording is started

Start/Stop Session Button after recording is started

Figure 2.35: Session Control Pane.

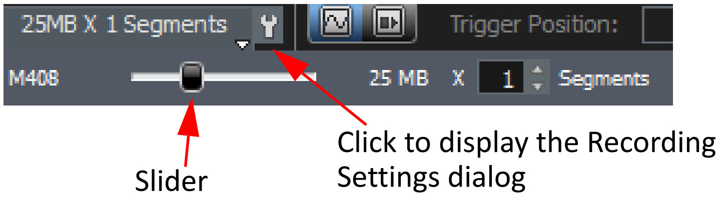
Disabling a port can be used to save recording buffer space. A disabled port can still trigger the analyzer.

Auto Speed is the default port speed selection. It will automatically detect and display the line speed. In rare cases (such as debugging speed negotiation), it might be desired to set the analyzers speed manually. Note, that when the speed is set manually, traffic at different speeds will not be captured correctly.

When “Trace is Not Saved” is displayed, this means that the trace is opened for viewing in Quick View mode, but it has not been saved to disk yet.

2.6.5 Recording Settings Pane

Use the Recording Settings (see Figure 2.36 on page 59) pane to select and set the number and size of segments and save a new trace file. (See “Buffer Size and Segments” on page 103.)



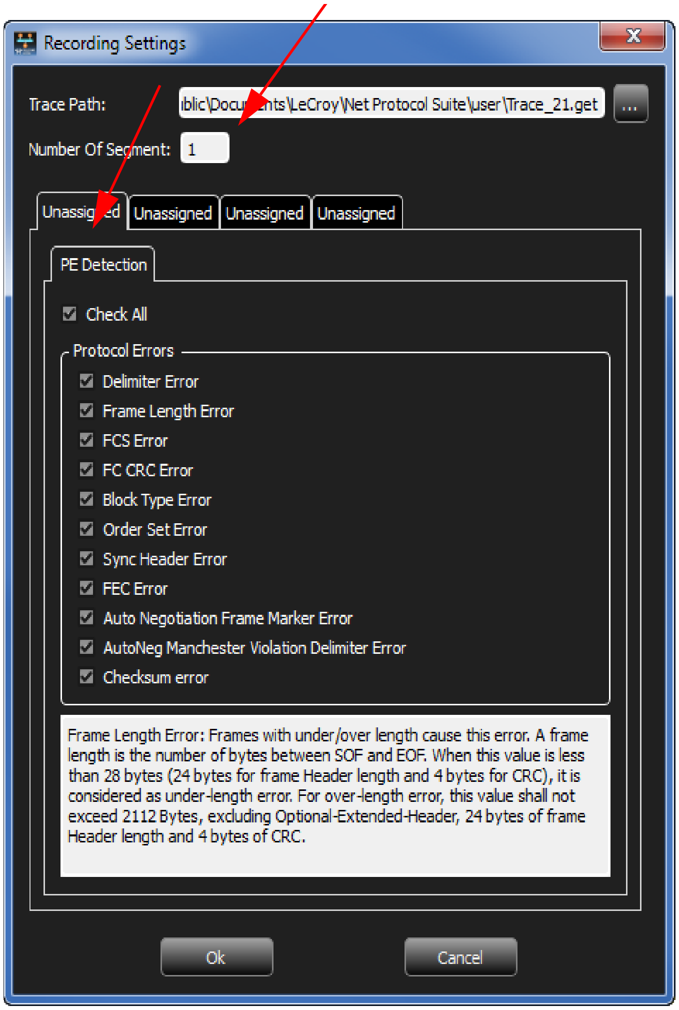
Slider

Click to display the Recording Settings dialog

Figure 2.36: Recording Settings Pane.

Protocol Error Detection

Click the Recording Settings icon to display the Recording Settings dialog. It has three tabs. In the GE 10G PE Detection Tab you can select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field.



Trace Path: ıblic\Documents\LeCroy\Net Protocol Suite\user\Trace_21.get

Number Of Segment: 1

☑ Check All

Protocol Errors

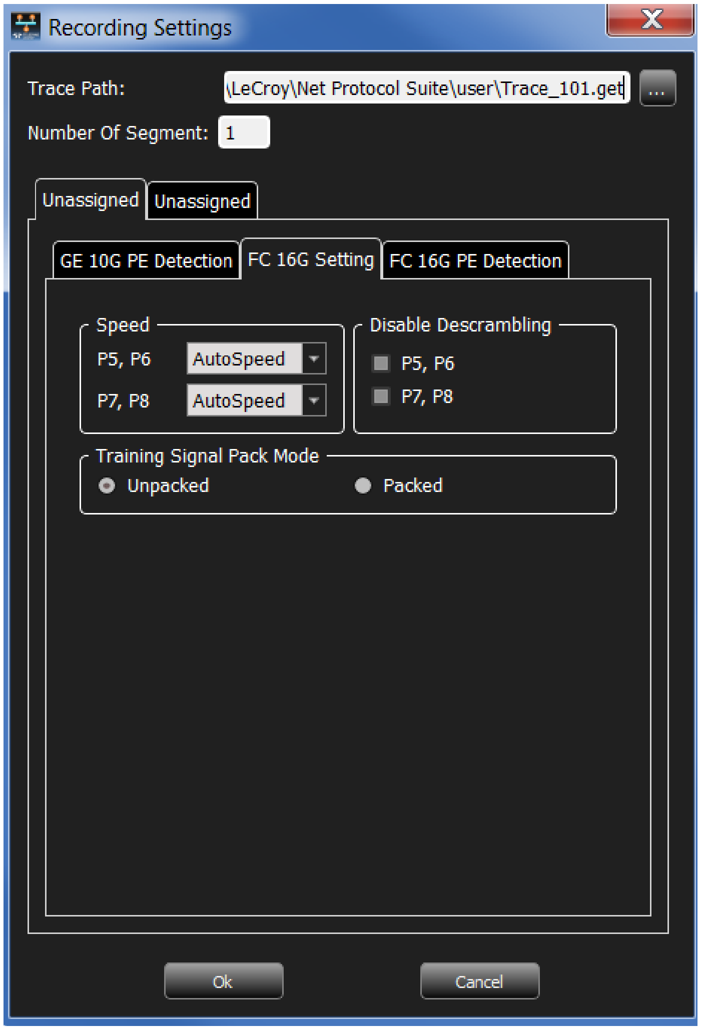
- ☑ Delimiter Error
- ☑ Frame Length Error
- ☑ FCS Error
- ☑ FC CRC Error
- ☑ Block Type Error
- ☑ Order Set Error
- ☑ Sync Header Error
- ☑ FEC Error
- ☑ Auto Negotiation Frame Marker Error
- ☑ AutoNeg Manchester Violation Delimiter Error
- ☑ Checksum error

Frame Length Error: Frames with under/over length cause this error. A frame length is the number of bytes between SOF and EOF. When this value is less than 28 bytes (24 bytes for frame Header length and 4 bytes for CRC), it is considered as under-length error. For over-length error, this value shall not exceed 2112 Bytes, excluding Optional-Extended-Header, 24 bytes of frame Header length and 4 bytes of CRC.

Figure 2.37: GE 10G PE Detection Tab - Recording Settings Dialog.

In the FC 16G Setting Tab you can select the following:

- ❑ Speed - select 1.0625, 2.125, 4.25. 8.5, 16.0 and Autospeed from the drop-down list. Autospeed is the default.
- ❑ Disable Descrambling - select ports.
- ❑ Training Signal Pack Mode - Unpacked and Packed.



Trace Path: \LeCroy\Net Protocol Suite\user\Trace_101.get

Number Of Segment: 1

Speed

P5, P6 AutoSpeed

P7, P8 AutoSpeed

Disable Descrambling

☐ P5, P6

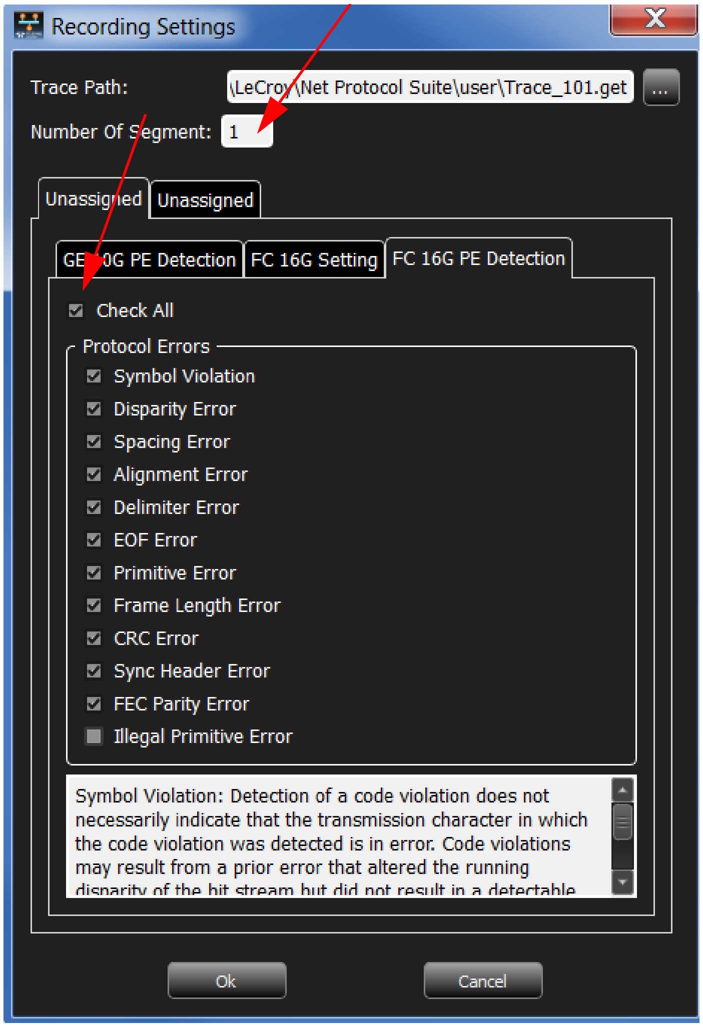
☐ P7, P8

Training Signal Pack Mode

● Unpacked ○ Packed

Figure 2.38: FC 16G Setting Tab - Recording Settings Dialog.

In the FC 16G PE Detection Tab, you can select which Protocol Errors the analyzer will show and which will be ignored. Select one or more protocol errors or select the **Check All** box to select all. Enter the Number of Segments in the field.



Trace Path: \LeCroy\Net Protocol Suite\user\Trace_101.get

Number Of Segment: 1

☑ Check All

Protocol Errors

☑ Symbol Violation
☑ Disparity Error
☑ Spacing Error
☑ Alignment Error
☑ Delimiter Error
☑ EOF Error
☑ Primitive Error
☑ Frame Length Error
☑ CRC Error
☑ Sync Header Error
☑ FEC Parity Error
☐ Illegal Primitive Error

Symbol Violation: Detection of a code violation does not necessarily indicate that the transmission character in which the code violation was detected is in error. Code violations may result from a prior error that altered the running disparity of the bit stream but did not result in a detectable

Figure 2.39: FC 16G PE Detection Tab - Recording Settings Dialog.

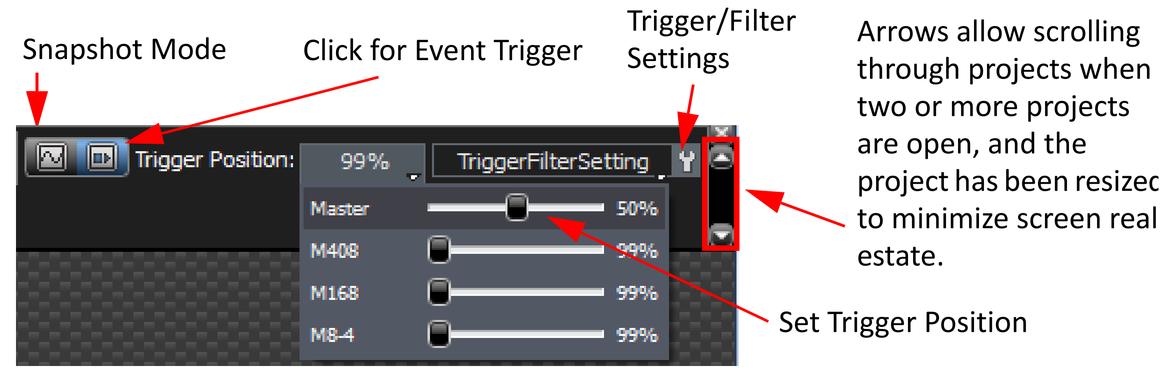
2.6.6 Trigger/Filter Settings Pane

Use the Trigger/Filter Settings pane to select Snapshot or Event Trigger mode and choose the Trigger Filter settings. The default mode is Snapshot. See “Trigger Filter Settings in Easy Mode” on page 64 for more information.

You can configure the following settings from this dialog:

- Select **New** from the dropdown menu to create new trigger filter settings. The Trigger Filter Settings dialog displays a name adding a new sequential Trigger Filter Setting. You can change the default name by typing a new name.
- Select **Manage** from the dropdown menu to manage the trigger filter settings (Choosing the Event Trigger option enables Trigger Position to set it manually. You can set the trigger position in the captured buffer as a percentage of the segment size. Trigger point of 0% means the trigger point will be on the first

packet in the buffer. (See “Trigger Position” on page 103.)



Snapshot Mode

Click for Event Trigger

Trigger/Filter Settings

Arrows allow scrolling through projects when two or more projects are open, and the project has been resizec to minimize screen real estate.

Set Trigger Position

Trigger Position: 99%

TriggerFilterSetting

Master	50%
M408	99%
M168	99%
M8-4	99%

Figure 2.40: Trigger/Filter Settings Pane.

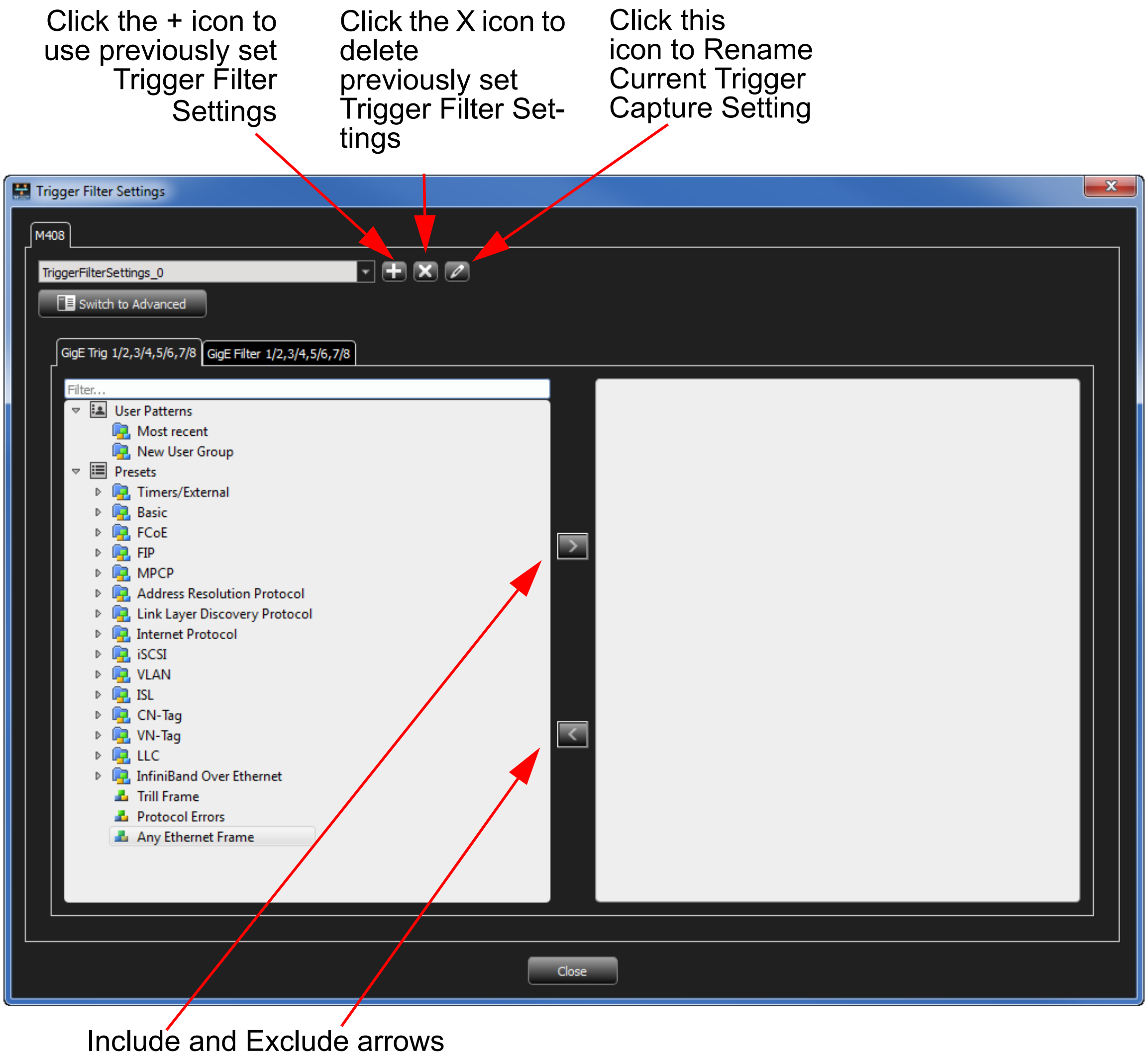
2.7 Trigger Filter Settings in Easy Mode

Easy mode allows you to operate the analyzer with minimum setup. In this mode, you can perform only a Trigger and Data capture. Use Easy Mode to get a comprehensive overview of your analyzer's capabilities.

The Trigger and Filter settings dialog allows you to set the parameters for triggering on selected triggers and filtering in (including) or filtering out (excluding) selected patterns. The dialog box opens with default settings to capture everything on the bus. The analyzer captures everything immediately without triggering on anything in particular.

2.7.1 Trigger Tab

You can drag and drop patterns from the Trigger Library pane into the Active Pane. You can select the pattern and use the Add and Remove arrows to move patterns between the Patterns Library and the Active pane (see Figure 2.41 on page 64). See "Trigger Setup" on page 101. You can copy a frame from the spreadsheet view and paste it in the Active Pane for triggering.



Click the + icon to use previously set Trigger Filter Settings

Click the X icon to delete previously set Trigger Filter Settings

Click this icon to Rename Current Trigger Capture Setting

Include and Exclude arrows

Figure 2.41: Trigger Settings Dialog.

Choose a Parameter

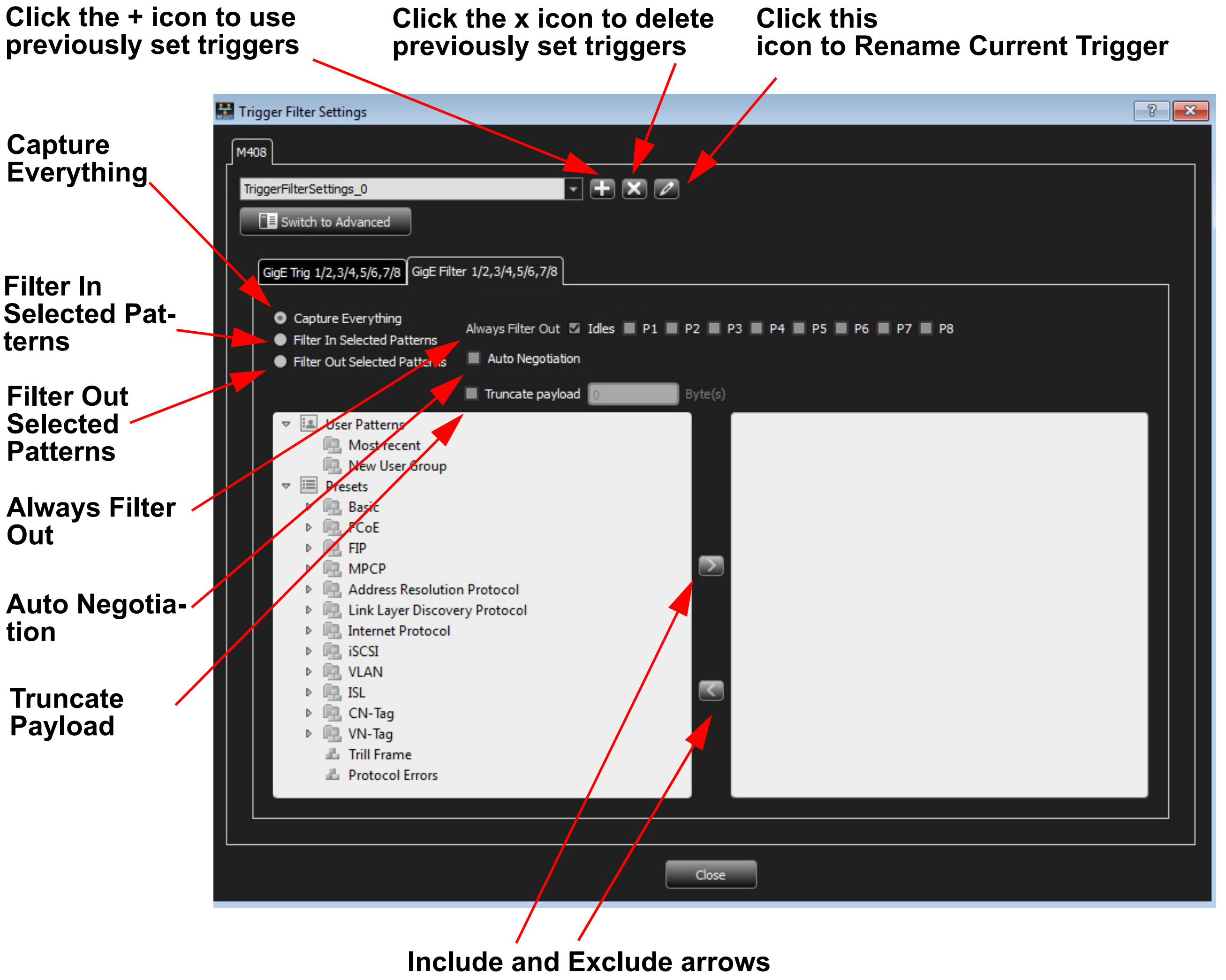
To choose a parameter for capture from any of these categories, highlight the category in the parameter window and click the **+>>** button to add the selection. You can also drag and drop a pattern. This opens selection dialogs for each of the categories displaying all of the parameters for that category. All patterns added appear in the Project Overview.

2.7.2 Filter Tab

You can drag and drop patterns from the Filter Library pane into the Active Pane. You can select the pattern and use the Add and Remove arrows to move patterns between the Patterns Library and the Active pane (see Figure 2.42). The following filtering options are available:

Capture Everything

Checking this option captures everything on the bus and the Pattern Library is greyed out (see figure below).



Click the + icon to use previously set triggers

Click the x icon to delete previously set triggers

Click this icon to Rename Current Trigger

Capture Everything

Filter In Selected Patterns

Filter Out Selected Patterns

Always Filter Out

Auto Negotiation

Truncate Payload

Include and Exclude arrows

Trigger Filter Settings
M408
TriggerFilterSettings_0
Switch to Advanced
GigE Trig 1/2,3/4,5/6,7/8
GigE Filter 1/2,3/4,5/6,7/8
● Capture Everything
○ Filter In Selected Patterns
○ Filter Out Selected Patterns
Always Filter Out ☑ Idles □ P1 □ P2 □ P3 □ P4 □ P5 □ P6 □ P7 □ P8
□ Auto Negotiation
□ Truncate payload 0 Byte(s)
User Patterns
Most recent
New User Group
Presets
Basic
FCoE
FIP
MPCP
Address Resolution Protocol
Link Layer Discovery Protocol
Internet Protocol
iSCSI
VLAN
ISL
CN-Tag
VN-Tag
Trill Frame
Protocol Errors
Close

Figure 2.42: Filter Dialog.

Filter in Selected Patterns

Checking this option includes the selected patterns in the trace capture (see Figure 2.42 on page 65).

Filter Out Selected Patterns

Checking this option excludes the selected patterns in the trace capture (see Figure 2.42 on page 65).

Always Filter Out

Check one or more option to exclude Idles and or P1 through P8 in the trace capture (see Figure 2.42 on page 65).

Note: Capturing a full buffer requires you to capture the traffic with all ports. Using four ports allows you to capture only half the system memory. The size of the system memory is based on the license purchased.

Auto Negotiation

Check this box to always filter out Auto Speed Negotiation traffic. (see Figure 2.42 on page 65).

Truncate Payload

Check this option to truncate payload after x-number of Dword(s) (see Figure 2.42 on page 65).

Note: For iSCSI packets, payload truncation may not truncate at the specified value as some packets could come out of sequence.

Run Hardware

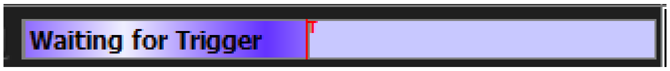
To get an immediate overview of the bus traffic to and from your Analyzer, click the ● **Start Session** button.

Recording Progress

The analyzer begins filling the defined memory buffer with traffic on the bus. After the traffic fills the memory buffer, the traffic is uploaded to the viewer. As recording progresses, the Session Controller indicator changes to reflect the recording progress graphically:

A red vertical line illustrates the location of the Trigger Position you selected in Trigger and Filter Settings.

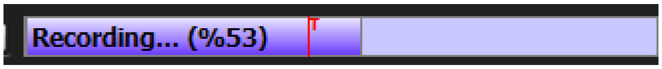
- ❑ Pre-Trigger progress is indicated by **Waiting for Trigger** in the field to the left of the Trigger Position.



Waiting for Trigger

Figure 2.43: Pre-Trigger.

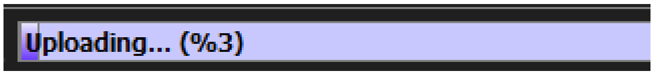
- ❑ After the trigger occurs **Recording** is displayed in the field to the left of the Trigger Position indicating the progress of the recording.



Recording... (%53)

Figure 2.44: Post-Trigger.

- ❑ When recording is complete **Uploading** is displayed indicating the progress of the data upload to the host machine.



Uploading... (%3)

Figure 2.45: Uploading.

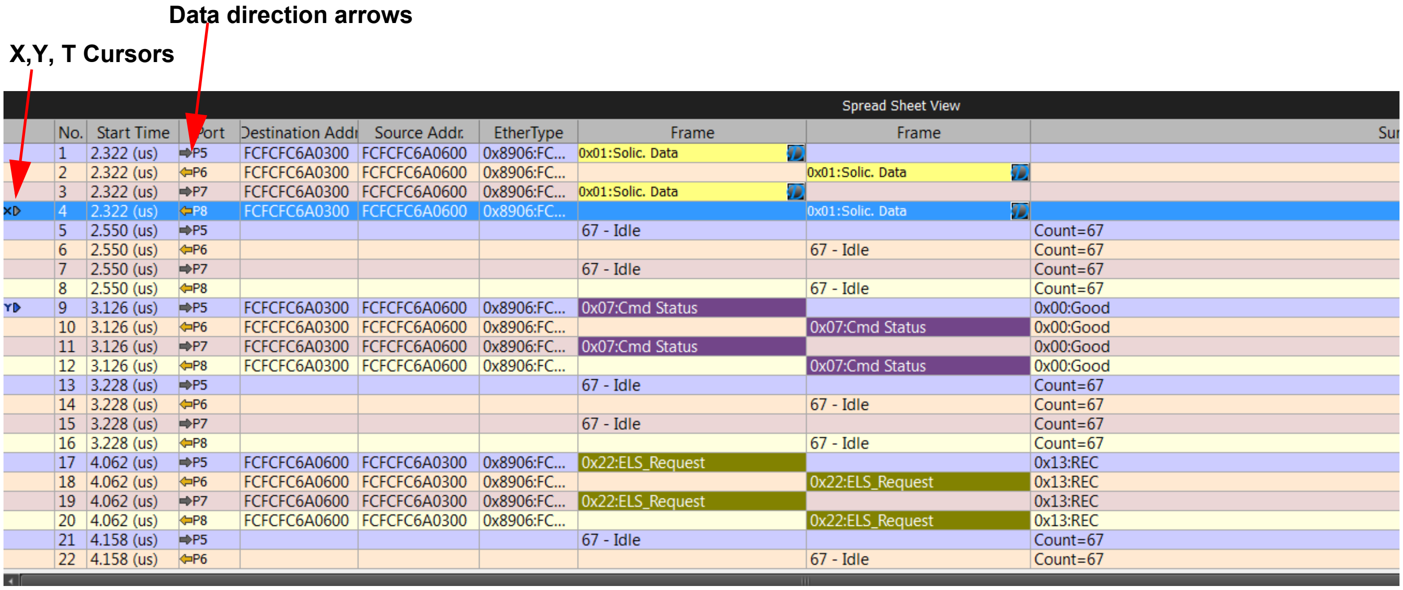
The Recorded Data file appears in the main display window.

Save the file for later use by selecting **File > Save**.

When a captured trace is not saved and the USB cable is removed, the software displays an error message that unsaved traces will be closed. If the user ignores the message, and again plugs in and unplugs the USB cable, the software might get into an unstable state.

When the Ethernet cable is removed, the application detects the event after a delay of approximately 2.5 to 3 minutes. During this delay the device status remains ready and an attempt to capture a trace might result in error messages such as :" PCI configuration failed", or " HAL error". If this occurs, you need to power cycle the analyzer to allow detecting the device in the device list and continue capturing.

Note: Spreadsheet View is the default display. However, you can view results in any of the different views by selecting **View** on the menu bar and choosing the desired View. The software remembers the last view (or views combination) used, and will automatically use that next time it is launched.



Spread Sheet View

	No.	Start Time	Port	Destination Addr	Source Addr.	EtherType	Frame	Frame	Sur
	1	2.322 (us)	⇨P5	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x01:Solic. Data		
	2	2.322 (us)	⇦P6	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x01:Solic. Data	
	3	2.322 (us)	⇨P7	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x01:Solic. Data		
X▷	4	2.322 (us)	⇦P8	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x01:Solic. Data	
	5	2.550 (us)	⇨P5				67 - Idle		Count=67
	6	2.550 (us)	⇦P6					67 - Idle	Count=67
	7	2.550 (us)	⇨P7				67 - Idle		Count=67
	8	2.550 (us)	⇦P8					67 - Idle	Count=67
Y▷	9	3.126 (us)	⇨P5	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x07:Cmd Status		0x00:Good
	10	3.126 (us)	⇦P6	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x07:Cmd Status	0x00:Good
	11	3.126 (us)	⇨P7	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x07:Cmd Status		0x00:Good
	12	3.126 (us)	⇦P8	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x07:Cmd Status	0x00:Good
	13	3.228 (us)	⇨P5				67 - Idle		Count=67
	14	3.228 (us)	⇦P6					67 - Idle	Count=67
	15	3.228 (us)	⇨P7				67 - Idle		Count=67
	16	3.228 (us)	⇦P8					67 - Idle	Count=67
	17	4.062 (us)	⇨P5	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...	0x22:ELS_Request		0x13:REC
	18	4.062 (us)	⇦P6	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...		0x22:ELS_Request	0x13:REC
	19	4.062 (us)	⇨P7	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...	0x22:ELS_Request		0x13:REC
	20	4.062 (us)	⇦P8	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...		0x22:ELS_Request	0x13:REC
	21	4.158 (us)	⇨P5				67 - Idle		Count=67
	22	4.158 (us)	⇦P6					67 - Idle	Count=67

Figure 2.46: Typical Spreadsheet View Results Display.

The results display shows each transaction for every layer identified in a different color and the data direction identified with data direction arrows. Upstream traffic has a solid yellow arrow from right to left: ⇐. Downstream traffic has a solid grey arrow left to right: ⇒.

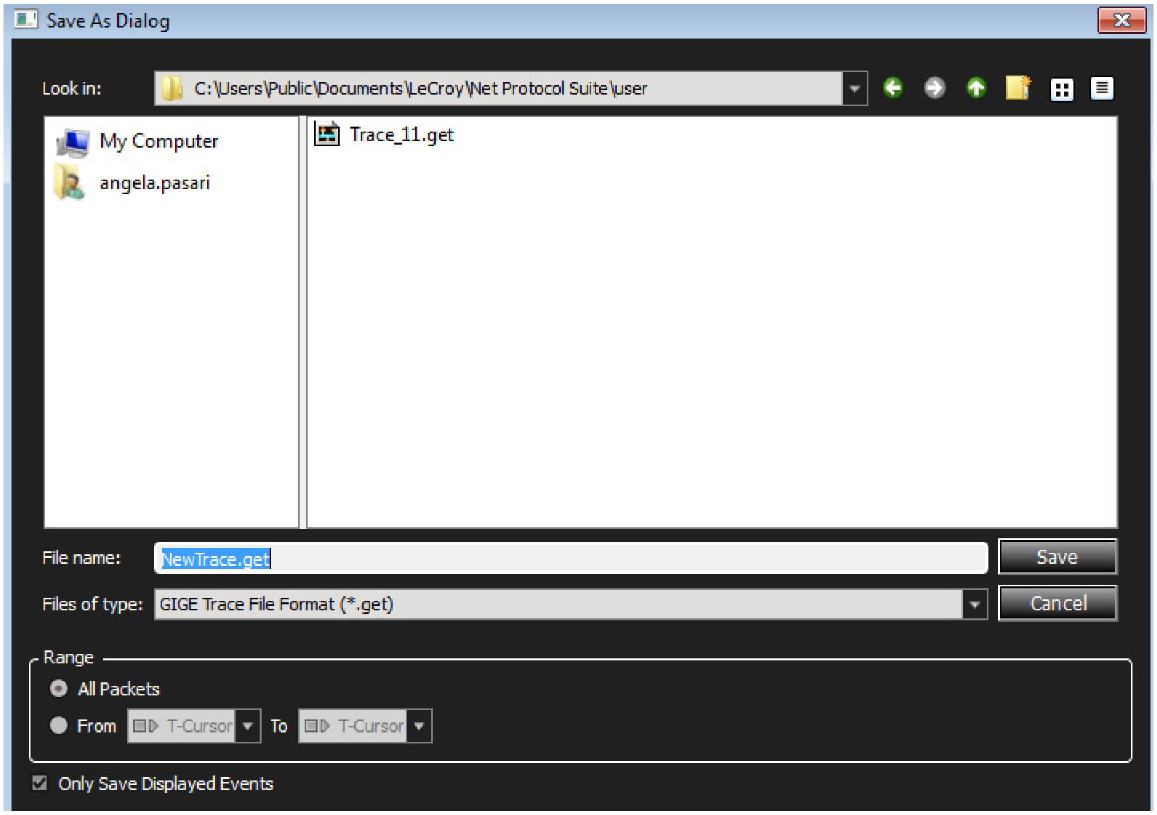
You can configure the viewer display for test and viewing preferences (see “Preferences” on page 149 for details about configuring the viewer display).

The Analysis Project dialog offers you a comprehensive set of choices to create a trigger and capture project satisfying some specific need. You can set the Analyzer to:

- Capture specific patterns (see “Patterns and Data Capture Setup” on page 71).
- Capture different patterns pre- and post-trigger (see “Patterns and Data Capture Setup” on page 71).
- Exclude parameters from capture (see “Patterns and Data Capture Setup” on page 71).
- Trigger on a pattern or sequence of patterns (see “Trigger Setup” on page 101).
- Configure trace capture memory
- Select file to save trace capture in memory

Saving a Trace Capture

You can save a Trace Capture for review at a later time using the **Save As** dialog.



Save As Dialog

Look in: C:\Users\Public\Documents\LeCroy\Net Protocol Suite\user

My Computer

angela.pasari

Trace_11.get

File name: NewTrace.get

Files of type: GIGE Trace File Format (*.get)

Range

● All Packets

○ From T-Cursor To T-Cursor

☑ Only Save Displayed Events

Figure 2.47: Save As Dialog.

You can limit the range of the saved file. You can save:

- All Packets

- A range between selected cursors
- A range between selected level of decoding. The levels allowed are dependent on the traffic in the trace. A trace with only Switch traffic might have the following levels available: ELS Cmd, Frame, GS Cmd, Sequence and SW Cmd, whereas a read-write trace might have Frame, SCSI Cmd and Sequence available.

Only Save Displayed Events: Click the checkbox to save only the Filtered in data in the trace.

Exporting a Trace Capture

You can export a Trace Capture by using the **Export** menu Option. Click **File > Export** and select from the three options.

You can:

- Export to Excel
- Export to Text
- Export and Open with Wireshark

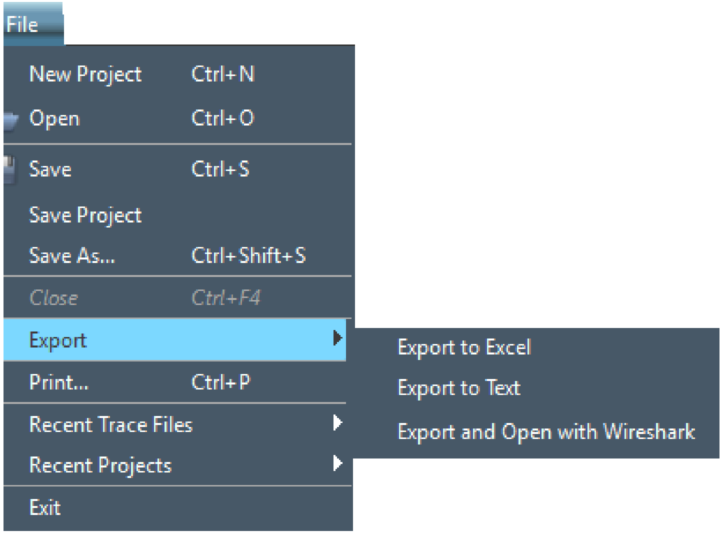


Figure 2.48: Export Dialog.

You can limit the range of the saved file. You can save:

- All Packets
- A range between selected cursors
- A range between selected level of decoding. The levels allowed are dependent on the traffic in the trace.

Project File Types

Projects have the following file types:

- *.gep Protocol Analyzer/Capture Project/Viewer file
- *.get Trace file
- *.xml Workspace file in Preferences

Example Projects

The Analyzer includes example projects that you can use to perform an immediate analysis without any setup.

The Analyzer system software has a pre-defined folder (directory) structure for storing all files. All example files are in the Examples folder under the SierraNet M408 Analyzer folder.

It is strongly recommended that you open some example files to see types of projects that you can create.

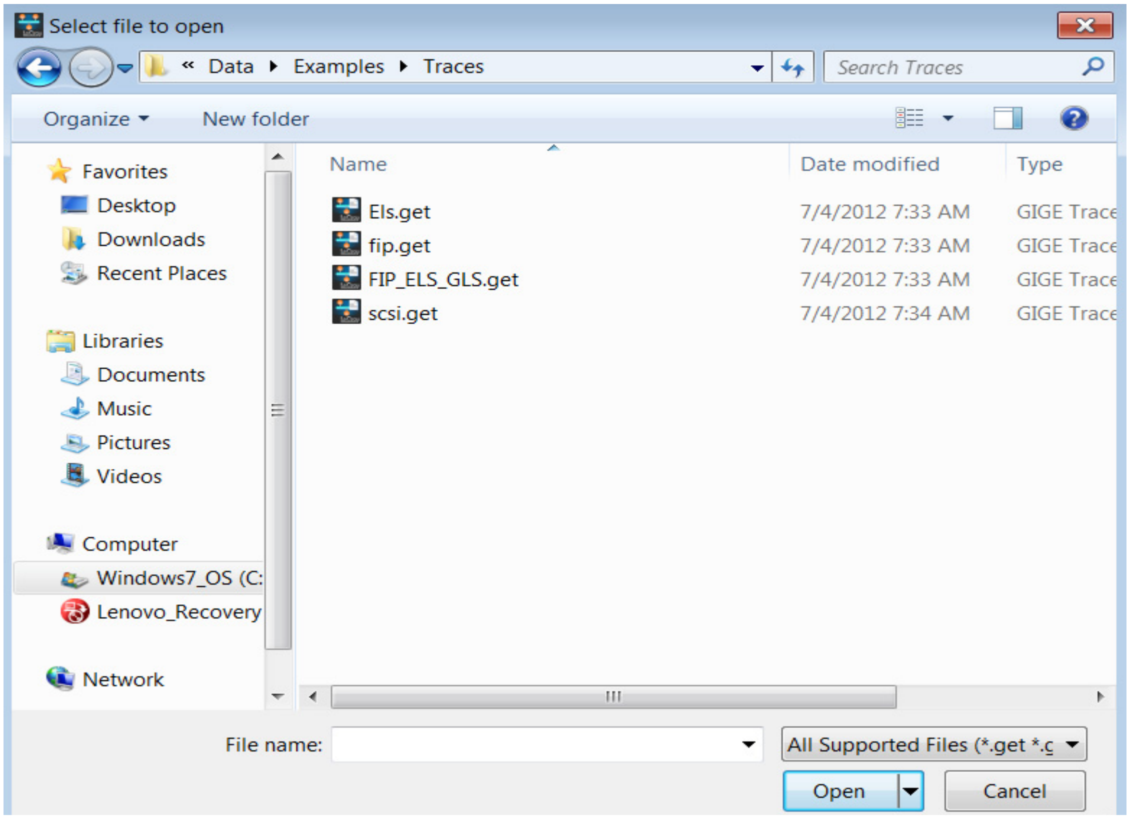
Run an Example Analysis Project

To run an example project:

1. Select **File > Open.**

   For Windows XP use - ROOT:\Program Files\LeCroy\Ethernet Protocol Suite

   For Windows Server2003 (32 bit), Windows Server 2012 (64 bit), Windows 7 or Windows 8 - ROOT:\Users\Public\Public Documents\LeCroy\Ethernet Protocol Suite
2. Locate example analysis projects by looking in the Examples folder. Traces are available and Traces. Click **Data > Examples > Traces**.
3. In the Traces folder, choose an example ***.get** file and click **Open** to display the example project dialog.



Name	Date modified	Type
Els.get	7/4/2012 7:33 AM	GIGE Trace
fip.get	7/4/2012 7:33 AM	GIGE Trace
FIP_ELS_GLS.get	7/4/2012 7:33 AM	GIGE Trace
scsi.get	7/4/2012 7:34 AM	GIGE Trace

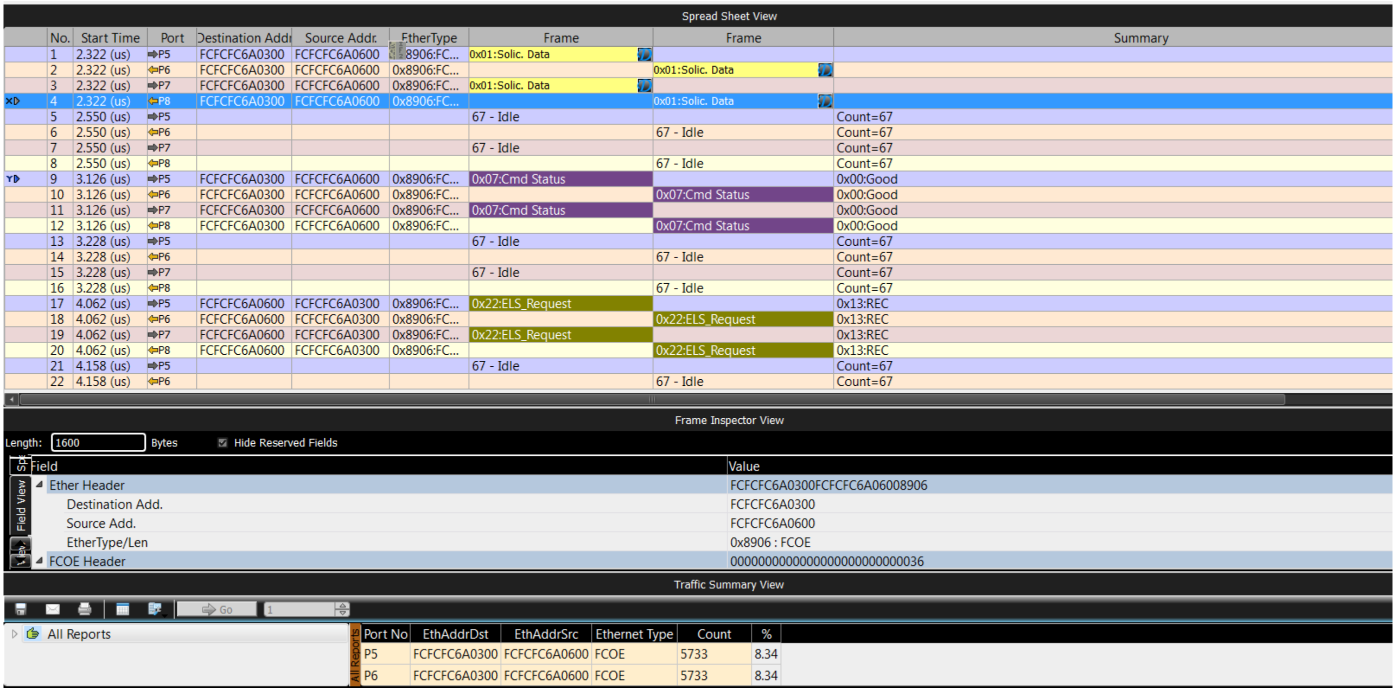
File name:

All Supported Files (*.get *.c

Figure 2.49: Open File Dialog.

4. Click the **Open** button to execute the pre-defined trace.

5. After the project runs, you see an analyzer trace capture display (see Figure 2.50 on page 71).



Spread Sheet View

	No.	Start Time	Port	Destination Addr	Source Addr.	EtherType	Frame	Frame	Summary
	1	2.322 (us)	⇨P5	FCFCFC6A0300	FCFCFC6A0600	8906:FC...	0x01:Solic. Data		
	2	2.322 (us)	⇦P6	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x01:Solic. Data	
	3	2.322 (us)	⇨P7	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x01:Solic. Data		
X▷	4	2.322 (us)	⇦P8	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x01:Solic. Data	
	5	2.550 (us)	⇨P5				67 - Idle		Count=67
	6	2.550 (us)	⇦P6					67 - Idle	Count=67
	7	2.550 (us)	⇨P7				67 - Idle		Count=67
	8	2.550 (us)	⇦P8					67 - Idle	Count=67
Y▷	9	3.126 (us)	⇨P5	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x07:Cmd Status		0x00:Good
	10	3.126 (us)	⇦P6	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x07:Cmd Status	0x00:Good
	11	3.126 (us)	⇨P7	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x07:Cmd Status		0x00:Good
	12	3.126 (us)	⇦P8	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x07:Cmd Status	0x00:Good
	13	3.228 (us)	⇨P5				67 - Idle		Count=67
	14	3.228 (us)	⇦P6					67 - Idle	Count=67
	15	3.228 (us)	⇨P7				67 - Idle		Count=67
	16	3.228 (us)	⇦P8					67 - Idle	Count=67
	17	4.062 (us)	⇨P5	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...	0x22:ELS_Request		0x13:REC
	18	4.062 (us)	⇦P6	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...		0x22:ELS_Request	0x13:REC
	19	4.062 (us)	⇨P7	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...	0x22:ELS_Request		0x13:REC
	20	4.062 (us)	⇦P8	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...		0x22:ELS_Request	0x13:REC
	21	4.158 (us)	⇨P5				67 - Idle		Count=67
	22	4.158 (us)	⇦P6					67 - Idle	Count=67

Frame Inspector View

Length: 1600 Bytes ☑ Hide Reserved Fields

Field	Value
◢ Ether Header	FCFCFC6A0300FCFCFC6A06008906
Destination Add.	FCFCFC6A0300
Source Add.	FCFCFC6A0600
EtherType/Len	0x8906 : FCOE
◢ FCOE Header	0000000000000000000000000036

Traffic Summary View

Port No	EthAddrDst	EthAddrSrc	Ethernet Type	Count	%
P5	FCFCFC6A0300	FCFCFC6A0600	FCOE	5733	8.34
P6	FCFCFC6A0300	FCFCFC6A0600	FCOE	5733	8.34

Figure 2.50: Analyzer Trace Capture Display.

For details about the results display, see “Display Manipulation” on page 113 and see “Preferences” on page 149.

2.7.3 Patterns and Data Capture Setup

You can refine data capture by choosing **Pattern** and then selecting specific patterns for capture. Additionally, you can define a different set of patterns to capture after trigger.

The Trigger and Filter settings dialog allows you to set the parameters for triggering on selected triggers and filtering in (including) or filtering out (excluding) selected patterns. Refer to “Trigger Filter Settings in Easy Mode” on page 64.

2.7.4 Pre- and Post Trigger Data Capture

Move the **Trigger Position** slider button (see Figure 2.40 on page 63) to define one set of patterns for capture prior to the occurrence of a trigger (left of the slider) and another set of patterns for capture after the occurrence of a trigger (right of the slider). The selection and setup procedure is the same for both Pre-Trigger capture and Post-Trigger capture. (see “Trigger Setup” on page 101).

2.7.5 Triggering/Filtering Patterns (Easy Mode)

The application provides User Patterns and a library of Preset patterns.

User Patterns

Recently used patterns are stored under the Most Recent user pattern.

Create a New User Group by right-clicking and selecting **New Group** as shown below. Key in the name of the new group.

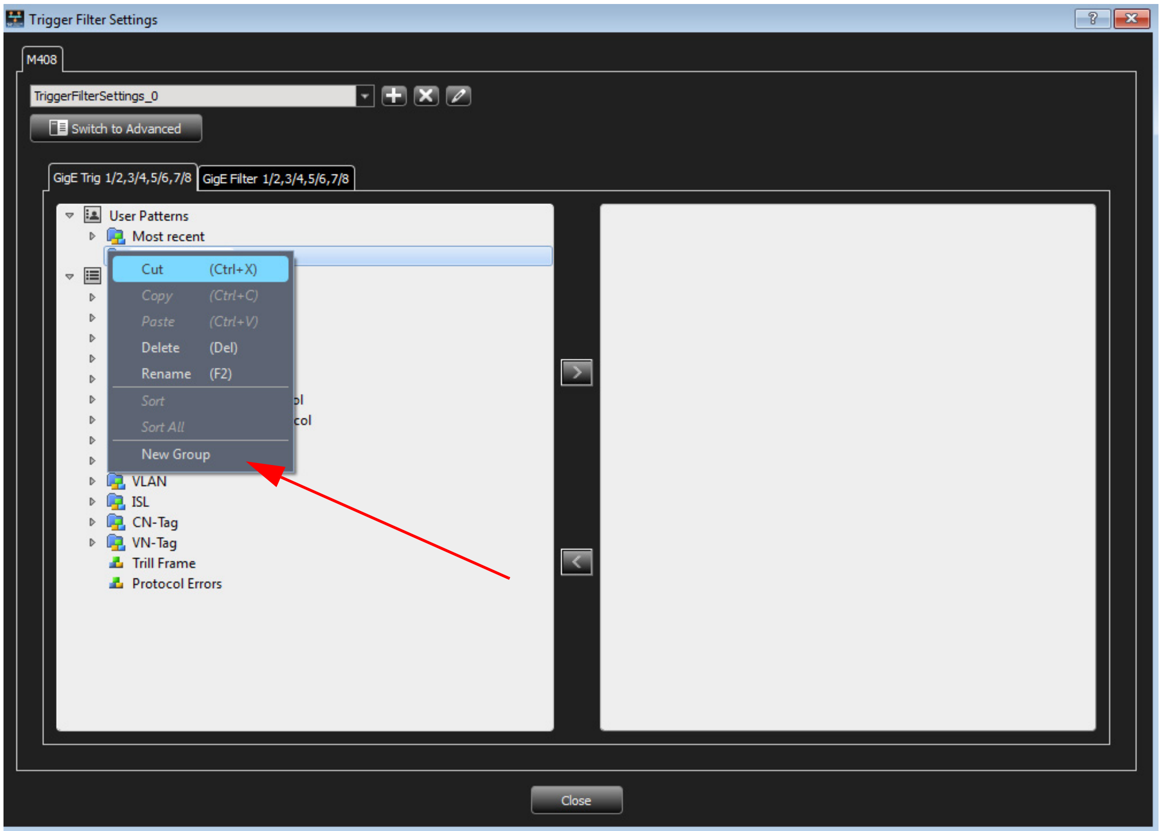


Figure 2.51: Creating a New User Group.

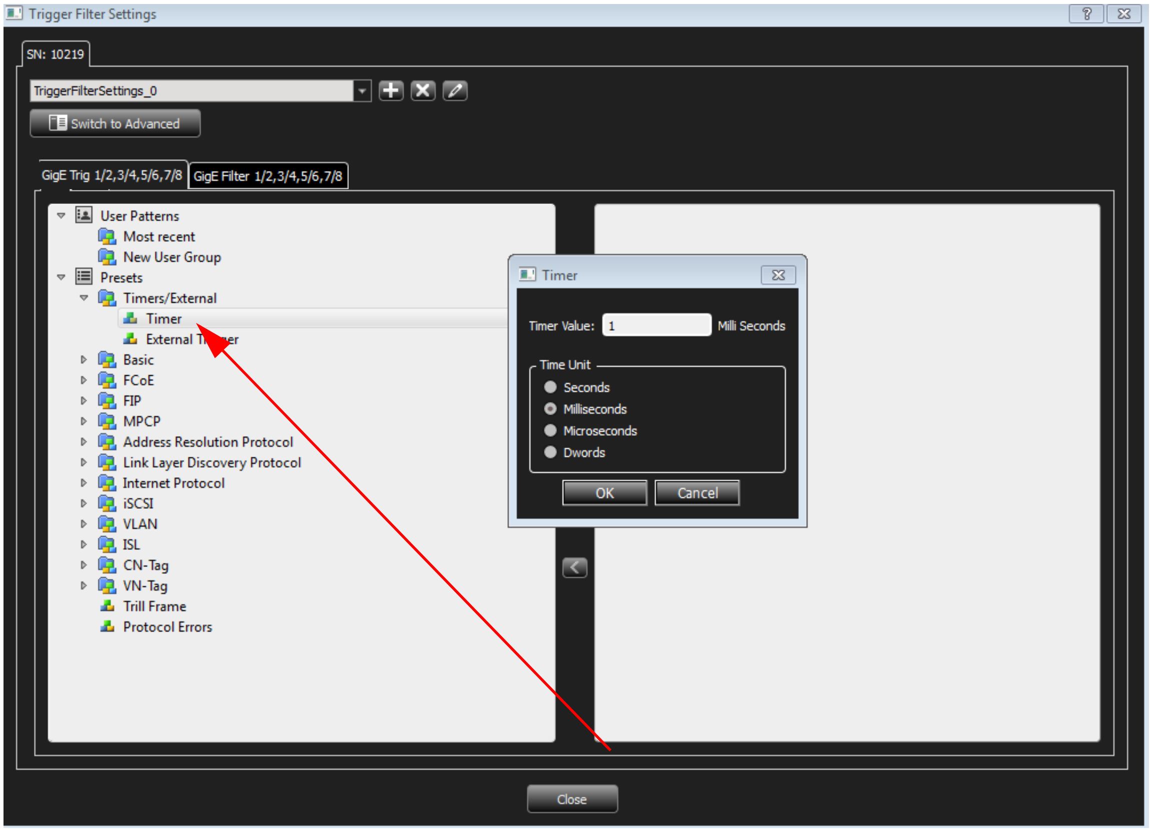
2.7.6 Timers/External

Timer

You can set a timer independently of any other trigger selection, to cause an unconditional trigger after a set time.

Double-click **Timer** in the Pattern window to open the Add Timer Pattern dialog.

Check a Time Unit, enter the Timer Value, and click **OK**.



Timer Value: 1 Milli Seconds

Time Unit
- ○ Seconds
- ● Milliseconds
- ○ Microseconds
- ○ Dwords

Figure 2.52: Timer Pattern Dialog.

Note: The timer resolution is limited to one DWORD. The minimum value is 12-13 DWORD.

External Trigger

Use this event to wait for a signal on the analyzers external trigger input. Refer to “External Trigger” on page 58 for details on configuring the external trigger input.

2.7.7 Pattern Editing Conventions

When entering values in patterns the following conventions apply:

In Binary, 'X' means one bit which is "don't care" and the value can be either 1 or 0. Below are some examples in binary and their meanings:

"X10": The value length is 3 bits and from right to left, the first and second bits have specific values and the third one is "don't care".

"XXXXXXX1": The value length is 8 bits and from right to left, the first bit has a specific value and the rest are "don't care".

In Hexadecimal 'X' means 4 bits in which all four are "don't care". In hexadecimal '?' means either one of the bits 1, 2, 3 or 4 bits is "don't care" and it is not clear which bit is "don't care" and which ones have specific value. Some examples are given in the table below.

Hexadecimal Value	Length in bits	Equivalent Value in Binary
"X1"	8 bits	"XXXX0001"
"X?"	8 bits	"XXXXXX10"
"?X"	8 bits	"110XXXXX"
"?"	2 bits	"XX"
"?"	3 bits	"11X"
"7"	3 bits	"111"
"7?"	8 bits	"01110XX1"

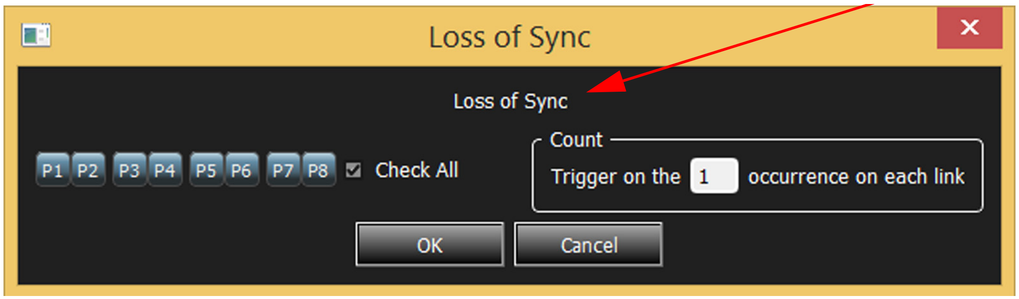
If VI_READ_RQST is selected, the value for the "Device HDR" field will be "10" in binary format as this field is a two-bits field. This field is the last field in the "DF_CTL" field which is an 8 bits field. For this specific frame, the value of "DF_CTL" will be "XXXXXX10" in binary format and "X?" in hexadecimal format according to the conventions above.

2.7.8 Ethernet Patterns

Basic

Loss of Sync

Double-click **Loss of Sync** to open the Loss of Sync Pattern dialog.



Loss of Sync

Loss of Sync

P1 P2 P3 P4 P5 P6 P7 P8 ☑ Check All

Count

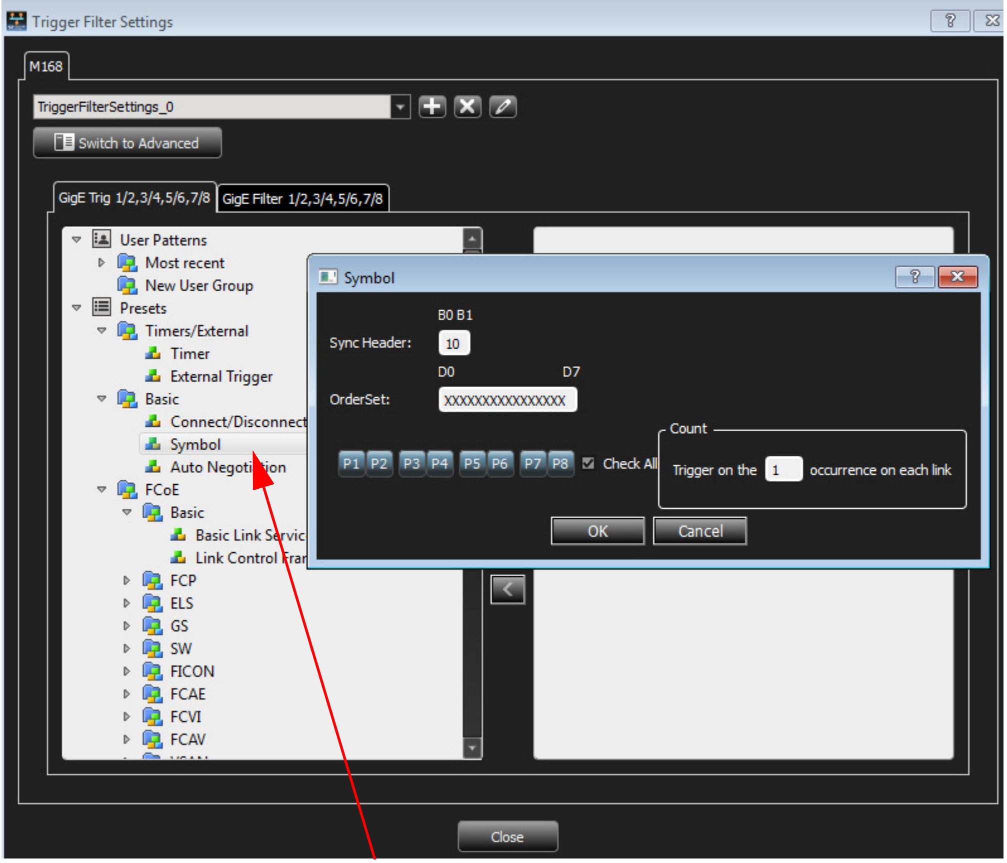
Trigger on the 1 occurrence on each link

Figure 2.53: Loss of Sync Pattern Dialog

This event detects loss of sync on the Ethernet physical layer receiver. Enter the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Symbol

Double-click **Symbol** to open the Symbol Pattern dialog.



Sync Header: 10

OrderSet: XXXXXXXXXXXXXXXX

☑ Check All

Trigger on the 1 occurrence on each link

Figure 2.54: Symbol Pattern Dialog

Enter the values for the Sync Header, Order Set and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Two different order sets can exist in one 64 bits payload of a 66 bits block. The six examples of a remote and local fault given below demonstrate how to manually enter ordered set triggers.

0x0100000001000055 -> local fault-local fault

0x000000000100004b -> local fault-idle

0x010000000000002D -> idle-local fault

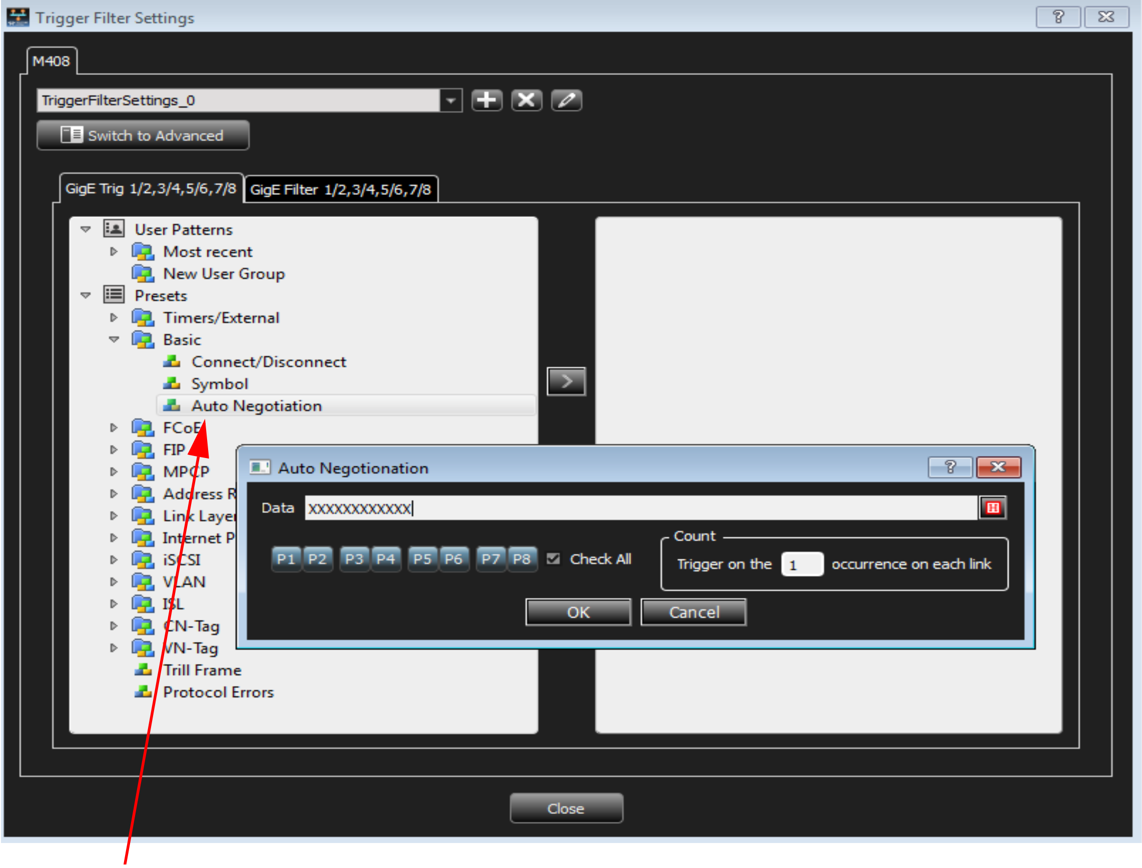
0x0200000002000055 -> remote fault-remote fault

0x000000000200004b -> remote fault-idle

0x020000000000002D -> idle-remote fault

Auto Negotiation

Double-click **Auto Negotiation** to open the Auto Negotiation Pattern dialog.



Data XXXXXXXXXXXX

☑ Check All

Count

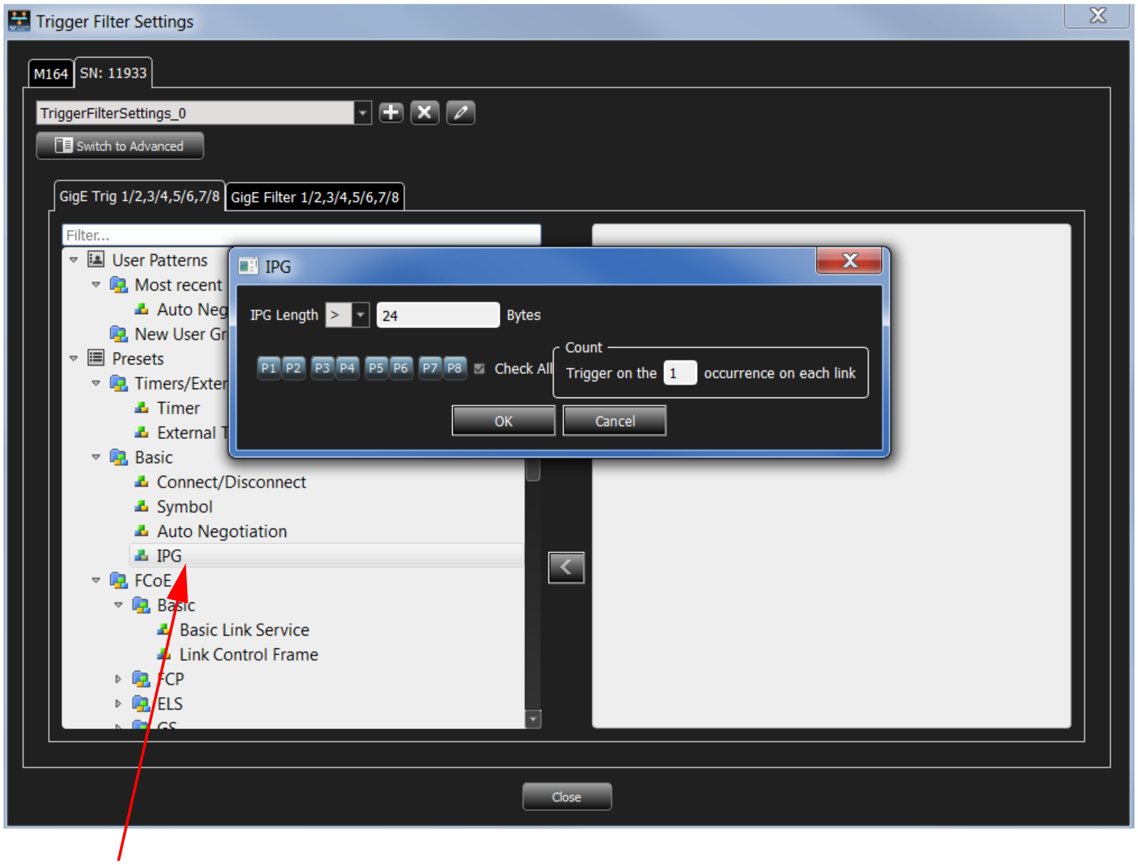
Trigger on the 1 occurrence on each link

Figure 2.55: Auto Negotiation Pattern Dialog

Enter the values for the Data, Code Word, Manchester and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

IPG

Double-click **IPG** to open the IPG dialog.



IPG Length > 24 Bytes

☑ Check All

Trigger on the 1 occurrence on each link

Figure 2.56: IPG Pattern Dialog

Enter the IPG Length from the drop-down list and Bytes values and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

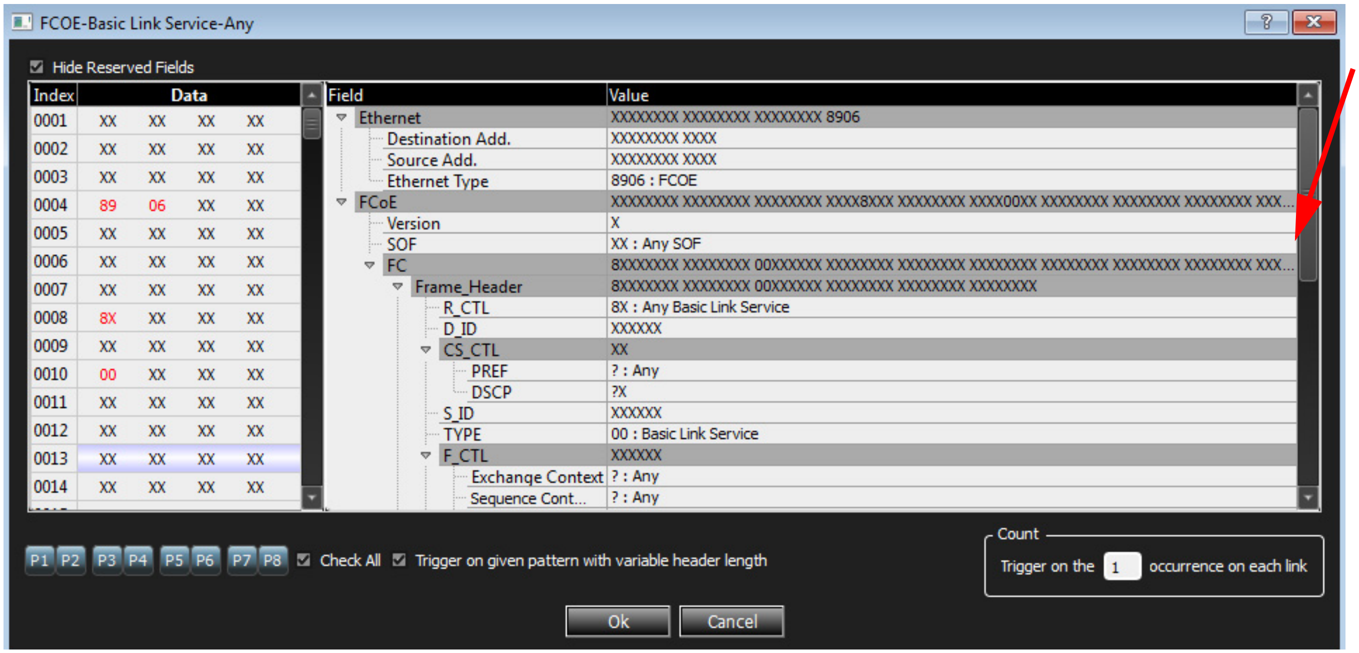
FCoE Patterns

Basic

Basic Link Service

For any Ethernet pattern, double-click the pattern name, for example, double-click **Basic Link Service** to open the Basic Link Service Pattern dialog.

Note: Some screen captures for the Ethernet patterns are similar to the screen capture shown below.



FCOE-Basic Link Service-Any

☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	89	06	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	8X	XX	XX	XX
0009	XX	XX	XX	XX
0010	00	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX 8906
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	8906 : FCOE
FCoE	XXXXXXXX XXXXXXXX XXXXXXXX XXXX8XXX XXXXXXXX XXXX00XX XXXXXXXX XXXXXXXX XXXXXXXX XXX...
Version	X
SOF	XX : Any SOF
FC	8XXXXXXX XXXXXXXX 00XXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXX...
Frame_Header	8XXXXXXX XXXXXXXX 00XXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
R_CTL	8X : Any Basic Link Service
D_ID	XXXXXX
CS_CTL	XX
PREF	? : Any
DSCP	?X
S_ID	XXXXXX
TYPE	00 : Basic Link Service
F_CTL	XXXXXX
Exchange Context	? : Any
Sequence Cont...	? : Any

☑ Check All ☑ Trigger on given pattern with variable header length

Count

Trigger on the 1 occurrence on each link

Figure 2.57: Basic Link Service Pattern Dialog

Enter the values for the Ethernet header, FCoE header, Frame header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

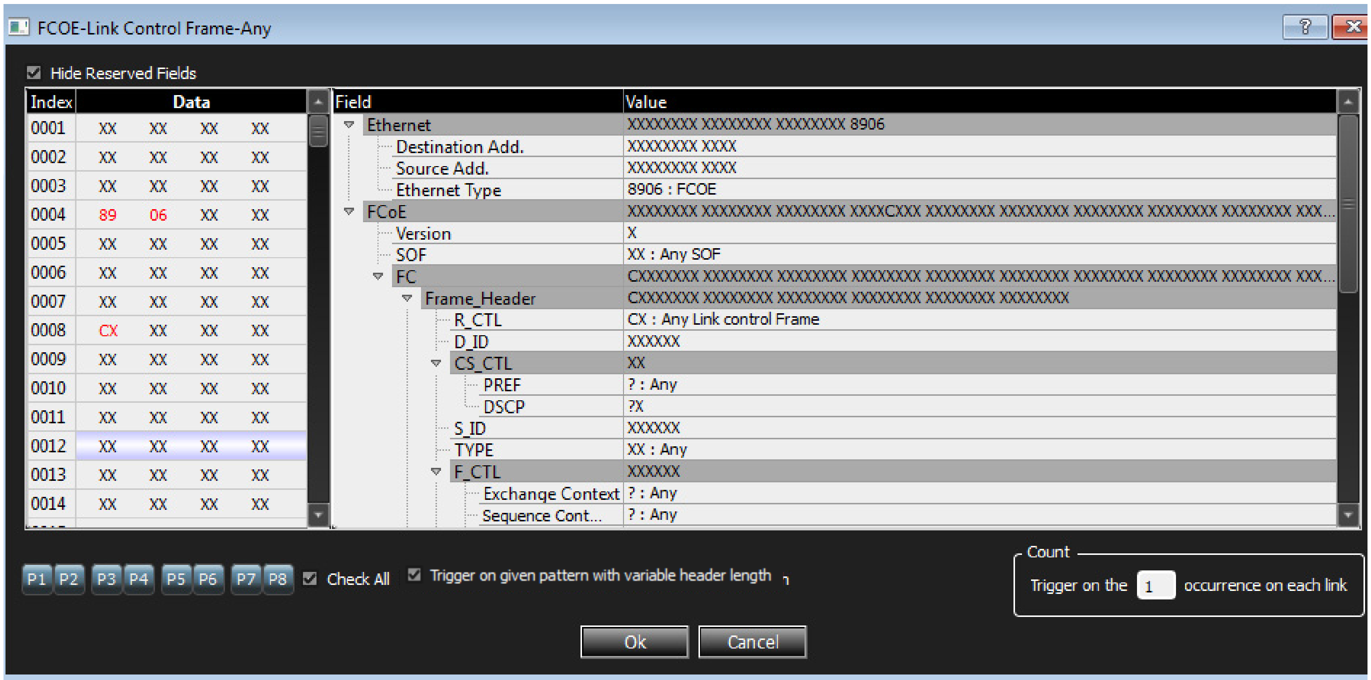
Check the **Trigger on given pattern with variable header length** box to automatically adjust the offset, if optional headers like VLAN tag, VNTag, etc. are present. Uncheck it, to trigger for a pattern at a specific offset from the start of the frame.

Note: Some patterns have additional options to select from drop-drown lists as shown in the figure above.

Link Control Frame

For any FCoE pattern, double-click the pattern name, for example, double-click **Basic Link Service** to open the Basic Link Service Pattern dialog.

Note: Some screen captures for the FCoE patterns are similar to the screen capture shown below.



FCOE-Link Control Frame-Any

☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	89	06	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	CX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX 8906
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	8906 : FCOE
FCoE	XXXXXXXX XXXXXXXX XXXXXXXX XXXXCXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXX...
Version	X
SOF	XX : Any SOF
FC	CXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXX...
Frame_Header	CXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
R_CTL	CX : Any Link control Frame
D_ID	XXXXXX
CS_CTL	XX
PREF	? : Any
DSCP	?X
S_ID	XXXXXX
TYPE	XX : Any
F_CTL	XXXXXX
Exchange Context	? : Any
Sequence Cont...	? : Any

☑ Check All ☑ Trigger on given pattern with variable header length

Count
Trigger on the 1 occurrence on each link

Figure 2.58: Link Control Frame Pattern Dialog

Enter the values for the Ethernet header, FCoE header, Frame header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Check the **Trigger on given pattern with variable header length** box to automatically adjust the offset, if optional headers like VLAN tag, VNTag, etc. are present. Uncheck it, to trigger for a pattern at a specific offset from the start of the frame.

The following additional Ethernet patterns are available:

FCP Patterns

Frame Information Unit

SCSI

Any SCSI Command

- 6-Byte Any SCSI Cmd
- 10-Byte Any SCSI Cmd
- 12-Byte Any SCSI Cmd
- 16-Byte Any SCSI Cmd
- Long LBA 16-Byte Any SCSI Cmd
- Variable Length Any SCSI Cmd
- Variable Length for Long LBA 32-Byte Any SCSI Cmd

- ❑ SPC4
- ❑ SBC3
- ❑ MMC6
- ❑ SMC2
- ❑ SSC2
- ❑ OSD2

- ❑ ADC3

FCP Task Management

ELS Patterns

ELS Request

ELS Reply

GS Patterns

Generic Link Service-Request

GS Reply

- ❑ GS_RJT
- ❑ GS Accept
  - ■ FC-SW-5
  - ■ Event Service
  - ■ Key Distribution Service
  - ■ Alias Service
  - ■ Management Service
    - Fabric Configuration Service
    - Unzoned Name Server
    - Fabric Zone Server
    - Reserved for Performance Server
    - Security Policy Server
    - Security Information Server
    - Fabric Device Management Server
  - ■ Time Service
  - ■ Directory Service -
    - Name Server
    - Directory Service - FC-4 Specific Servers

SW Patterns

SW Request

SW Reply

FICON Patterns

FCAE Patterns

FCAE_ASM

FCAE-1553

FCVI Patterns

FCAV Patterns

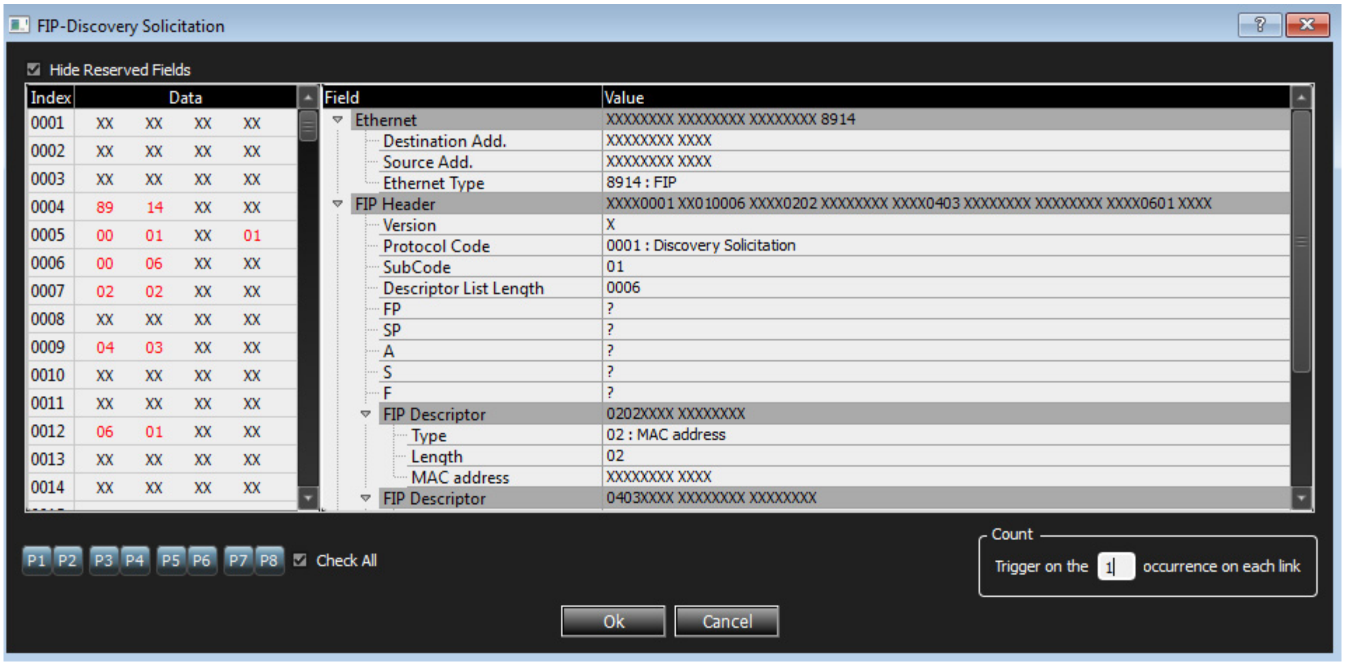
VSAN Patterns

(all FC patterns listed above are available under VSAN as well)

FIP Patterns

For any FIP pattern, double-click the pattern name, for example, double-click **Discovery Solicitation from ENode** to open the dialog.

Note: All the screen captures for the FIP patterns are similar to the screen capture shown below.



FIP-Discovery Solicitation

☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	89	14	XX	XX
0005	00	01	XX	01
0006	00	06	XX	XX
0007	02	02	XX	XX
0008	XX	XX	XX	XX
0009	04	03	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	06	01	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX 8914
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	8914 : FIP
FIP Header	XXXX0001 XX010006 XXXX0202 XXXXXXXX XXXX0403 XXXXXXXX XXXXXXXX XXXX0601 XXXX
Version	X
Protocol Code	0001 : Discovery Solicitation
SubCode	01
Descriptor List Length	0006
FP	?
SP	?
A	?
S	?
F	?
FIP Descriptor	0202XXXX XXXXXXXX
Type	02 : MAC address
Length	02
MAC address	XXXXXXXX XXXX
FIP Descriptor	0403XXXX XXXXXXXX XXXXXXXX

P1 P2 P3 P4 P5 P6 P7 P8 ☑ Check All

Count

Trigger on the 1 occurrence on each link

Figure 2.59: FIP Discovery Solicitation from ENode Pattern Dialog

Enter the values for the Ether header, FIP Header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

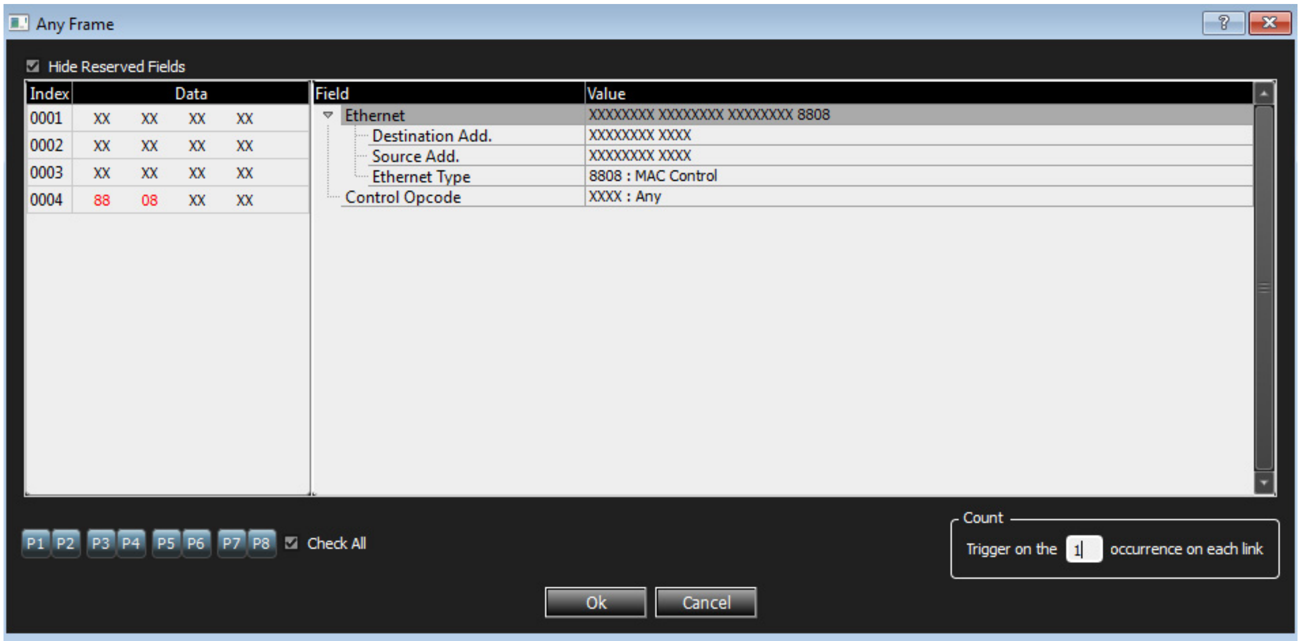
The following FIP patterns are available:

- ❑ Discovery Solicitation from ENode
- ❑ Discovery Solicitation from FCF
- ❑ Discovery Advertisement
- ❑ FIP FLOGI Request
- ❑ FIP FLOGI LS_ACC
- ❑ FIP FLOGI LS_RJT
- ❑ FIP NPIV FDISC Request
- ❑ FIP NPIV FDISC LS_ACC
- ❑ FIP NPIV FDISC LS_RJT
- ❑ FIP Fabric LOGO
- ❑ FIP Fabric LOGO LS_ACC
- ❑ FIP Fabric LOGO LS_RJT
- ❑ FIP ELP Request
- ❑ FIP ELP SW_ACC
- ❑ FIP ELP SW_RJT
- ❑ FIP Keep Alive

- ❑ FIP Clear Virtual Links-5DWORD Descriptor
- ❑ FIP VLAN Request-2DWORD Descriptor
- ❑ FIP VLAN Notification

MPCP Pattern

Double-click **Multi control Protocol Frame** to open the dialog.



Any Frame

☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	88	08	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX 8808
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	8808 : MAC Control
Control Opcode	XXXX : Any

☑ Check All

Count

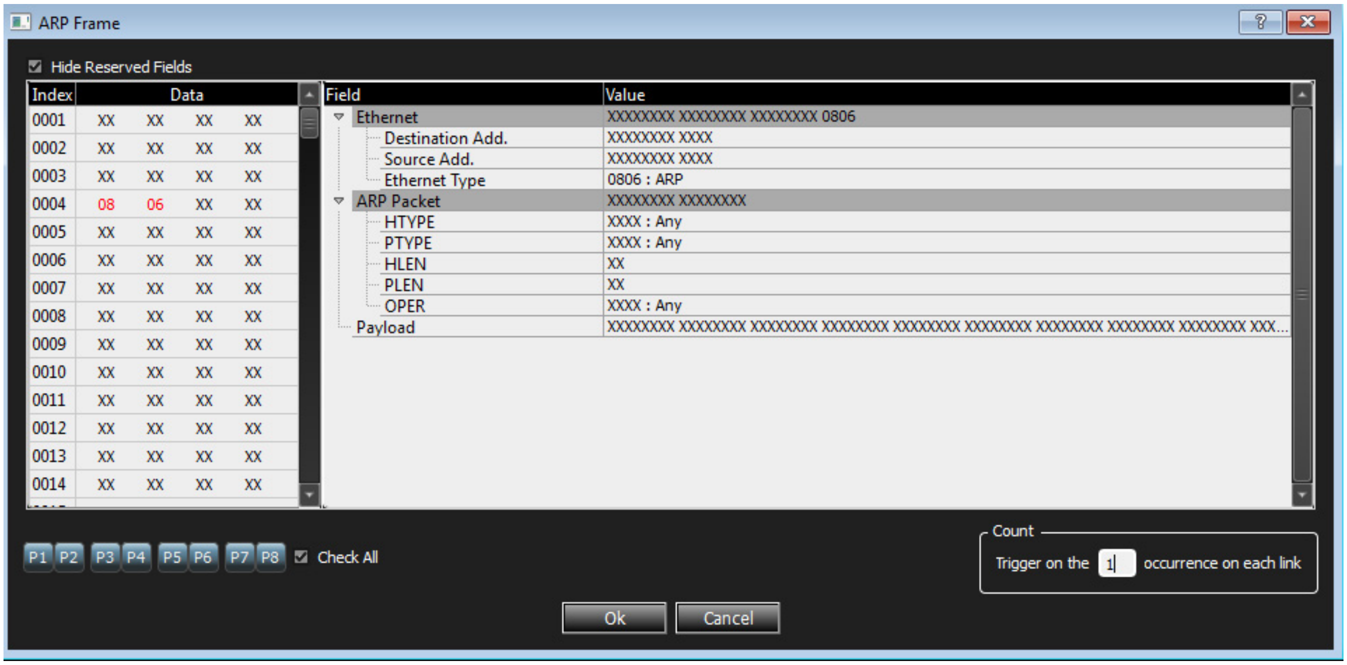
Trigger on the 1 occurrence on each link

Figure 2.60: Multi control Protocol Frame Pattern Dialog

Enter the values for the Ether header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Address Resolution Protocol Pattern

Double-click **Address Resolution Protocol** to open the dialog.



☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	08	06	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX 0806
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	0806 : ARP
ARP Packet	XXXXXXXX XXXXXXXX
HTYPE	XXXX : Any
PTYPE	XXXX : Any
HLEN	XX
PLEN	XX
OPER	XXXX : Any
Payload	XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXX...

☑ Check All

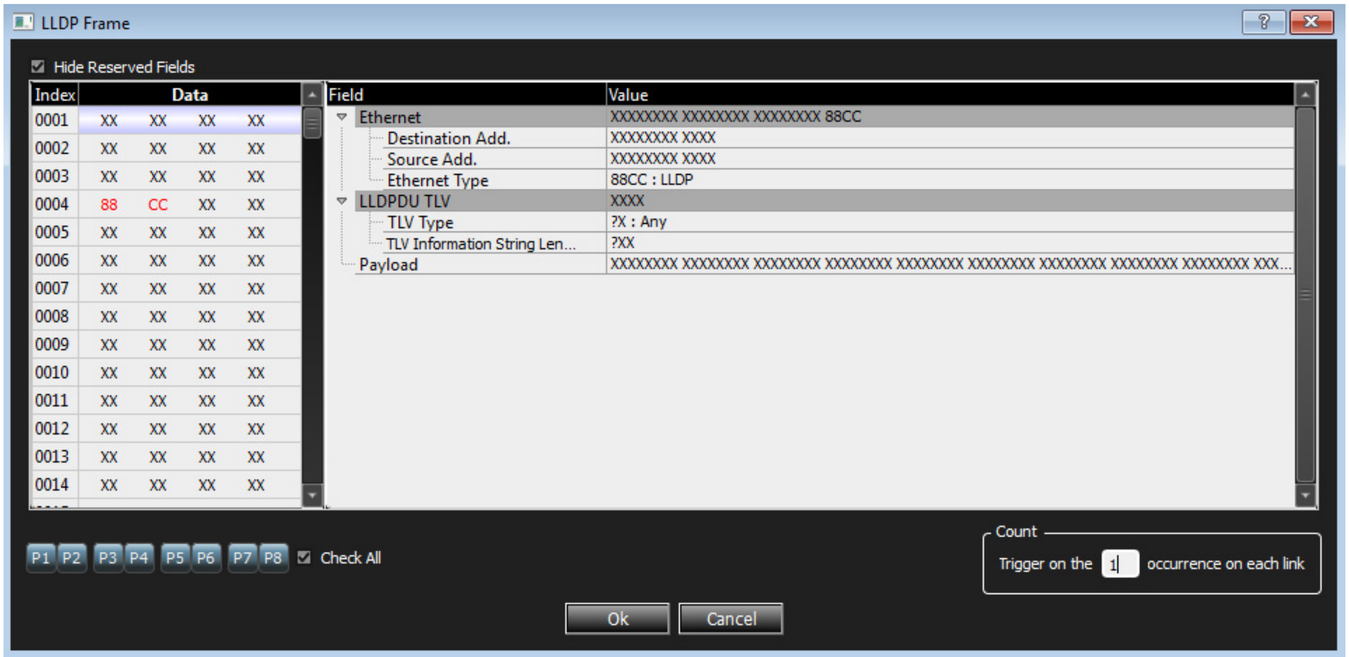
Count
Trigger on the 1 occurrence on each link

Figure 2.61: ARP Frame Dialog

Enter the values for the Ether header, ARP Packet and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Link Layer Discovery Protocol Pattern

Double-click **LLDP Frame** to open the dialog.



☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	88	CC	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX 88CC
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	88CC : LLDP
LLDPDU TLV	XXXX
TLV Type	?X : Any
TLV Information String Len...	?XX
Payload	XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXX...

☑ Check All

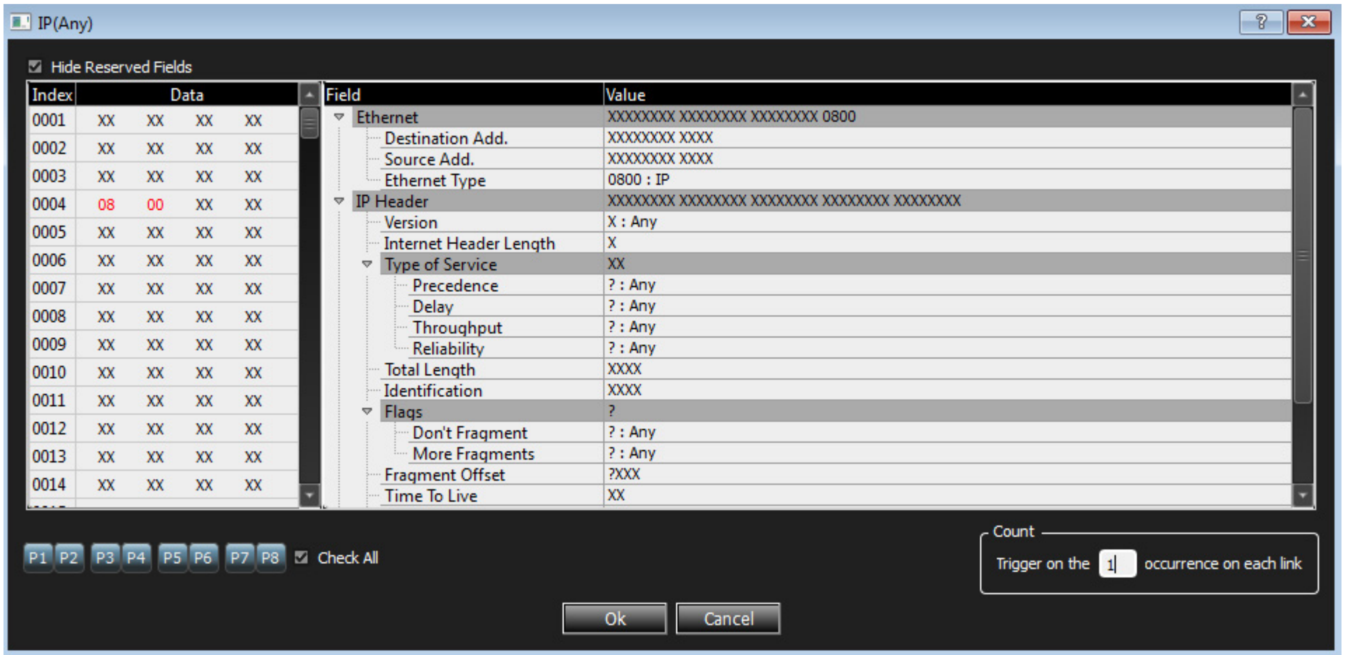
Count
Trigger on the 1 occurrence on each link

Figure 2.62: LLDP Frame Dialog

Enter the values for the Ether header, LLDPDU TLV and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Internet Protocol Pattern

Double-click **Any IP Frame** to open the dialog.



Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	08	00	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX 0800
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	0800 : IP
IP Header	XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
Version	X : Any
Internet Header Length	X
Type of Service	XX
Precedence	? : Any
Delay	? : Any
Throughput	? : Any
Reliability	? : Any
Total Length	XXXX
Identification	XXXX
Flags	?
Don't Fragment	? : Any
More Fragments	? : Any
Fragment Offset	?XXX
Time To Live	XX

Count

Trigger on the 1 occurrence on each link

Figure 2.63: IP Frame Dialog

Enter the values for the Ether header, IP Header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

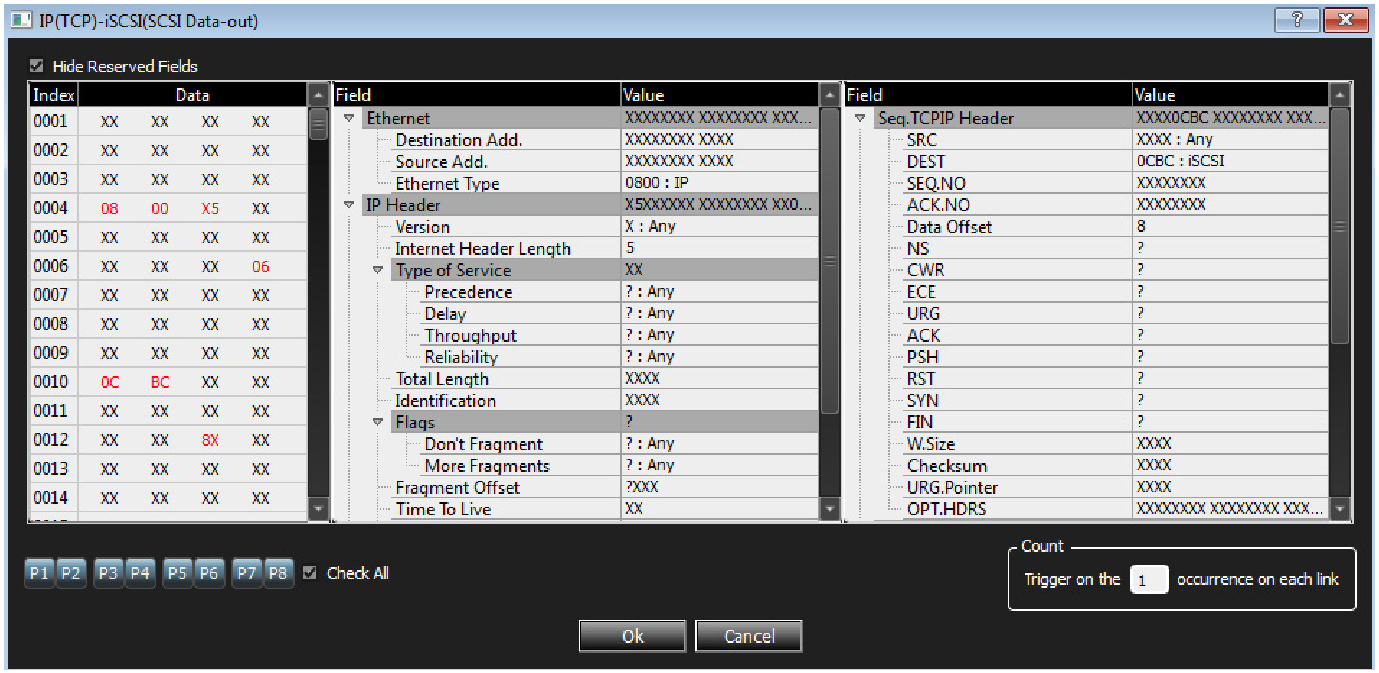
Other Internet Protocol patterns available are:

- IP Frame (ICMP)
- IP Frame (IGMP)
- IP Frame (IPV6)
- IP Frame (OSPF)
- IP Frame (AH)
- IP Frame (ESP)
- IP Frame (PIM)
- IP Frame (UDP)
- IP Frame (TCP)

iSCSI Pattern

Initiator PDU

Double-click **iSCSI Data-Out** to open the dialog.



IP(TCP)-iSCSI(SCSI Data-out)

☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	08	00	X5	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	06
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	0C	BC	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	8X	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXX...
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	0800 : IP
IP Header	X5XXXXXX XXXXXXXX XX0...
Version	X : Any
Internet Header Length	5
Type of Service	XX
Precedence	? : Any
Delay	? : Any
Throughput	? : Any
Reliability	? : Any
Total Length	XXXX
Identification	XXXX
Flags	?
Don't Fragment	? : Any
More Fragments	? : Any
Fragment Offset	?XXX
Time To Live	XX

Field	Value
Seq.TCPIP Header	XXXX0CBC XXXXXXXX XXX...
SRC	XXXX : Any
DEST	0CBC : iSCSI
SEQ.NO	XXXXXXXX
ACK.NO	XXXXXXXX
Data Offset	8
NS	?
CWR	?
ECE	?
URG	?
ACK	?
PSH	?
RST	?
SYN	?
FIN	?
W.Size	XXXX
Checksum	XXXX
URG.Pointer	XXXX
OPT.HDRS	XXXXXXXX XXXXXXXX XXX...

Count: Trigger on the 1 occurrence on each link

Figure 2.64: iSCSI Data-Out Dialog

Enter the values for the Ether header, IP Header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Other ISCSI patterns available are:

- iSCSI Login Request
- iSCSI Logout Request
- iSCSI NOP-Out
- iSCSI SNACK Request
- iSCSI Task Mgmt Request
- iSCSI Text Request

Target PDU

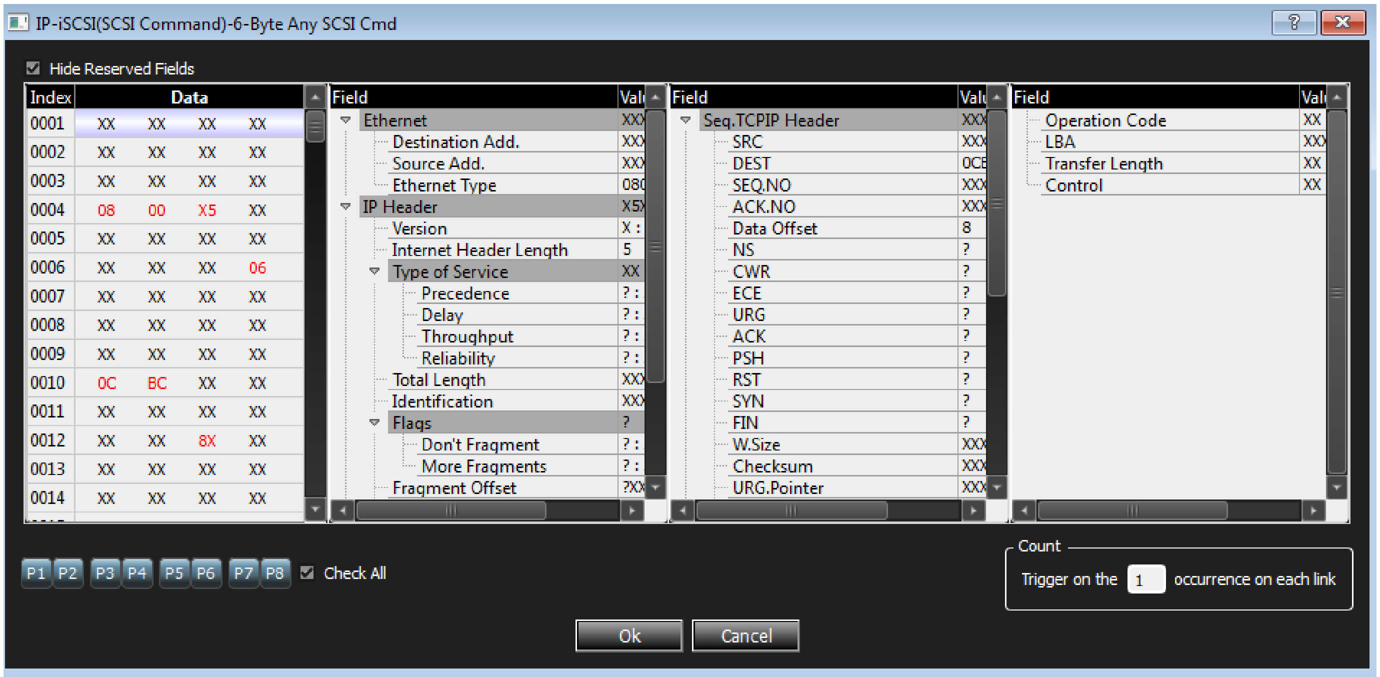
The dialogs are similar to the Initiator PDU above. The patterns available are:

- iSCSI Asynchronous Message
- iSCSI Response
- iSCSI Data-In
- iSCSI Login Response
- iSCSI Logout Response
- iSCSI Nop-In
- iSCSI Ready to Transfer
- iSCSI Reject
- iSCSI Task Mgmt Request
- iSCSI Text Request

ISCSI Cmd

Any SCSI Command

Double-click **6-Byte Any SCSI Cmd** to open the dialog.



IP-iSCSI(SCSI Command)-6-Byte Any SCSI Cmd

☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	08	00	X5	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	06
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	0C	BC	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	8X	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Valu
Ethernet	XXX
Destination Add.	XXX
Source Add.	XXX
Ethernet Type	080
IP Header	X5X
Version	X :
Internet Header Length	5
Type of Service	XX
Precedence	? :
Delay	? :
Throughput	? :
Reliability	? :
Total Length	XXX
Identification	XXX
Flags	?
Don't Fragment	? :
More Fragments	? :
Fragment Offset	?XX

Field	Valu
Seq.TCPIP Header	XXX
SRC	XXX
DEST	0CB
SEQ.NO	XXX
ACK.NO	XXX
Data Offset	8
NS	?
CWR	?
ECE	?
URG	?
ACK	?
PSH	?
RST	?
SYN	?
FIN	?
W.Size	XXX
Checksum	XXX
URG.Pointer	XXX

Field	Valu
Operation Code	XX
LBA	XXX
Transfer Length	XX
Control	XX

☑ Check All

Count

Trigger on the 1 occurrence on each link

Figure 2.65: 6-Byte Any SCSI Cmd Dialog

Enter the values for the Ether header, IP Header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Other ISCSI patterns available are:

- 10-Byte Any SCSI Cmd
- 12-Byte Any SCSI Cmd
- 16-Byte Any SCSI Cmd
- Long LBA16-Byte Any SCSI Cmd
- Variable Length Any SCSI Cmd
- Variable Length For Long LBA 32-Byte Any SCSI Cmd

- SPC4
- SBC3
- MMC6
- SMC2
- SSC2
- OSD2
- ADC3

iWARP Patterns

You may set patterns for the following iWARP RDMA operations:

Write

Read Request

Read Response

Send

Send with Invalidate

Send with SE

Send with SE and Invalidate

Terminate

VLAN Patterns

All Ethernet Patterns are available as VLAN Patterns as well. The only difference is that the Ethernet Type of the Ethernet header will be preset to "VLAN", and you should specify the VLAN id value in the VLAN Tag header.

VXLAN Patterns

All Ethernet Patterns are available as VXLAN Patterns as well. The only difference is that the frame will be preset as an IP/UDP frame with the UDP destination port set to "VXLAN", and you should specify the VXLAN Network Id in the VXLAN header.

ISL Patterns

FCoE

All the ISL FCoE patterns are similar to Ethernet patterns. Refer to "FCoE Patterns" on page 77.

FIP

All the ISL FIP patterns are similar to FIP patterns. Refer to "FIP Patterns" on page 81.

MPCP

All the ISL MPCP patterns are similar to MPCP patterns. Refer to "MPCP Pattern" on page 82.

Address Resolution Protocol

The ISL Address Resolution Protocol pattern is similar to Address Resolution Protocol pattern. Refer to "Address Resolution Protocol Pattern" on page 82.

Link Layer Discovery Protocol

The ISL Link Layer Discovery Protocol pattern is similar to Link Layer Discovery Protocol pattern. Refer to "Link Layer Discovery Protocol Pattern" on page 83.

ISL Internet Protocol

All the ISL Internet Protocol patterns are similar to Internet Protocol patterns. Refer to "Internet Protocol Pattern" on page 84.

iSCSI Pattern

All the ISL ISCSI patterns are similar to ISCSI patterns. Refer to "iSCSI Pattern" on page 84.

Initiator PDU

See "Initiator PDU" on page 84.

Target PDU

See "Target PDU" on page 85.

iSCSI Cmd

See "ISCSI Cmd" on page 86.

Note: For all ISL patterns enter a value for the ISL Header.

InfiniBand Over Ethernet (IBXoE)

See "InfiniBand Over Ethernet (IBXoE)" on page 89.

CN Tag Patterns

All the CN Tag patterns are similar to Ethernet patterns. Refer to "FCoE Patterns" on page 77.

Note: For all CN Tag patterns enter a value for CN Tag.

VN Tag Patterns

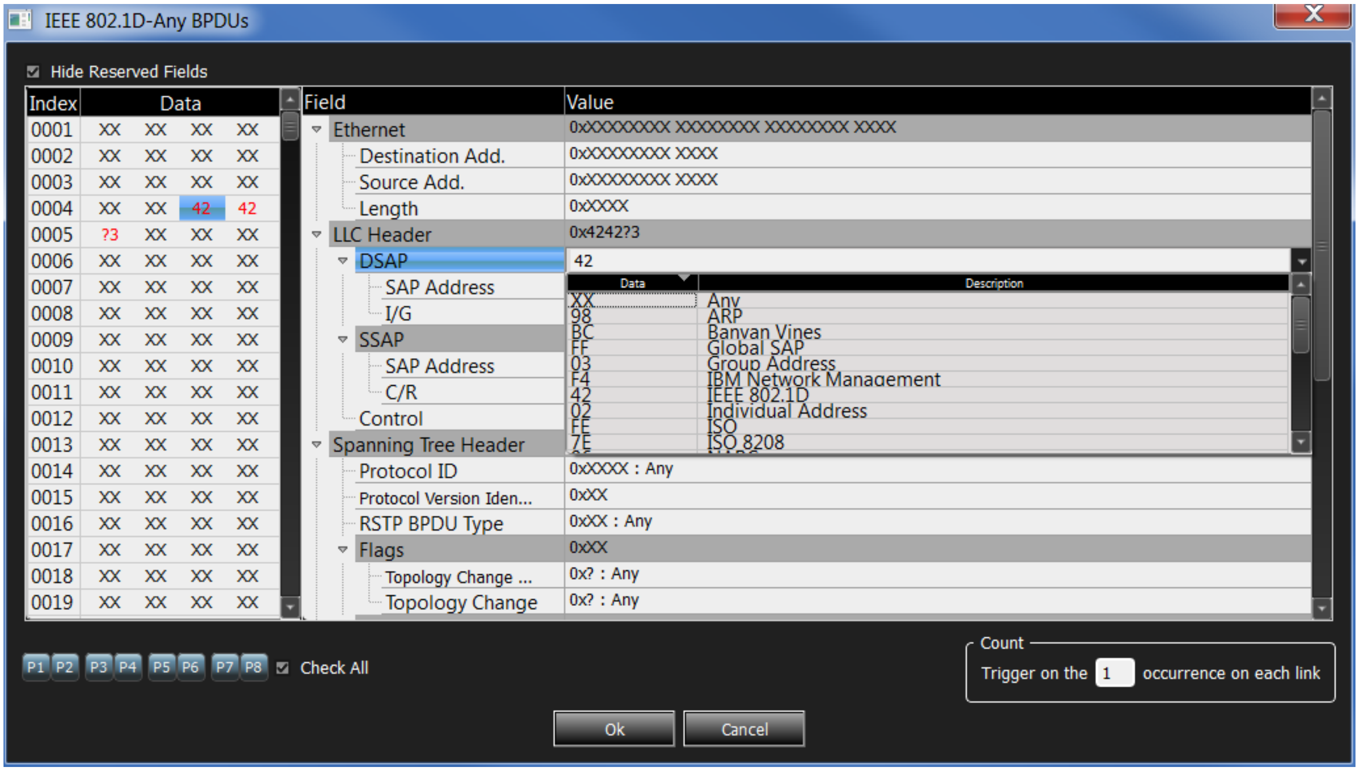
All the VN Tag patterns are similar to Ethernet patterns. Refer to "FCoE Patterns" on page 77.

Note: For all VN Tag patterns enter a value for VN Tag.

LLC

LLC-IEEE802.1D Frame

Double-click **LLC-IEEE802.1D** Frame to open the dialog.



IEEE 802.1D-Any BPDUs

☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	XX	XX	42	42
0005	?3	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX
0015	XX	XX	XX	XX
0016	XX	XX	XX	XX
0017	XX	XX	XX	XX
0018	XX	XX	XX	XX
0019	XX	XX	XX	XX

Field	Value
Ethernet	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXX
Destination Add.	0xXXXXXXXX XXXX
Source Add.	0xXXXXXXXX XXXX
Length	0xXXXX
LLC Header	0x4242?3
DSAP	42
SAP Address	
I/G	
SSAP	
SAP Address	
C/R	
Control	
Spanning Tree Header	
Protocol ID	0xXXXX : Any
Protocol Version Iden...	0xXX
RSTP BPDU Type	0xXX : Any
Flags	0xXX
Topology Change ...	0x? : Any
Topology Change	0x? : Any

Data	Description
XX	Any
98	ARP
BC	Banyan Vines
FF	Global SAP
03	Group Address
F4	IBM Network Management
42	IEEE 802.1D
02	Individual Address
FE	ISO
7E	ISO 8208

☑ Check All

Count

Trigger on the 1 occurrence on each link

Figure 2.66: LLC-IEEE802.1D Dialog

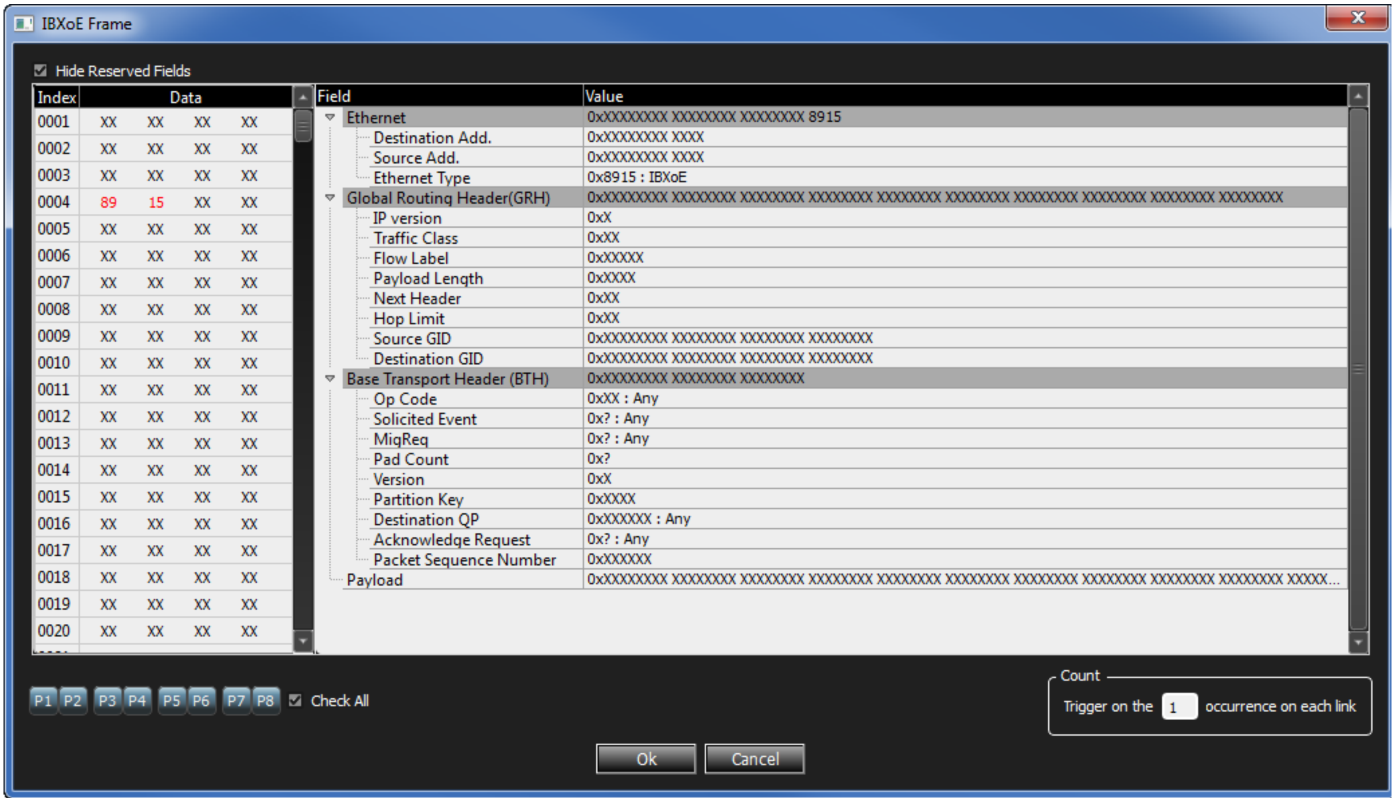
Enter the values for the Ethernet, LLC Header, Spanning Tree Header, GARP Header and select an option from the DSAP and SSAP pull -down menus. Enter the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Other LLC-IEEE802.1D patterns available are:

- ■ Bridge Protocol Data Unit (BPDU)
- ■ Configuration BPDUs
- ■ Multiple Spanning Tree BPDUs (MSTP)
- ■ Rapid Spanning Tree BPDUs (RSTP)
- ■ Topology Change Notification BPDU (TCNP)
- ❑ GARP Multicast Registration Protocol (GMRP)
- ❑ GARP VLAN Registration Protocol (GVRP)
- ❑ Generic Attribute Registration Protocol (GARP)

InfiniBand Over Ethernet (IBXoE)

Double-click **InfiniBand Over Ethernet (IBXoE)** to open the IBXoE Frame dialog.



☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	89	15	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX
0015	XX	XX	XX	XX
0016	XX	XX	XX	XX
0017	XX	XX	XX	XX
0018	XX	XX	XX	XX
0019	XX	XX	XX	XX
0020	XX	XX	XX	XX

Field	Value
Ethernet	0xXXXXXXXX XXXXXXXX XXXXXXXX 8915
Destination Add.	0xXXXXXXXX XXXX
Source Add.	0xXXXXXXXX XXXX
Ethernet Type	0x8915 : IBXoE
Global Routing Header(GRH)	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
IP version	0xX
Traffic Class	0xXX
Flow Label	0xXXXXX
Payload Length	0xXXXX
Next Header	0xXX
Hop Limit	0xXX
Source GID	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
Destination GID	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
Base Transport Header (BTH)	0xXXXXXXXX XXXXXXXX XXXXXXXX
Op Code	0xXX : Any
Solicited Event	0x? : Any
MigReq	0x? : Any
Pad Count	0x?
Version	0xX
Partition Key	0xXXXX
Destination QP	0xXXXXXX : Any
Acknowledge Request	0x? : Any
Packet Sequence Number	0xXXXXXX
Payload	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXX...

☑ Check All

Count

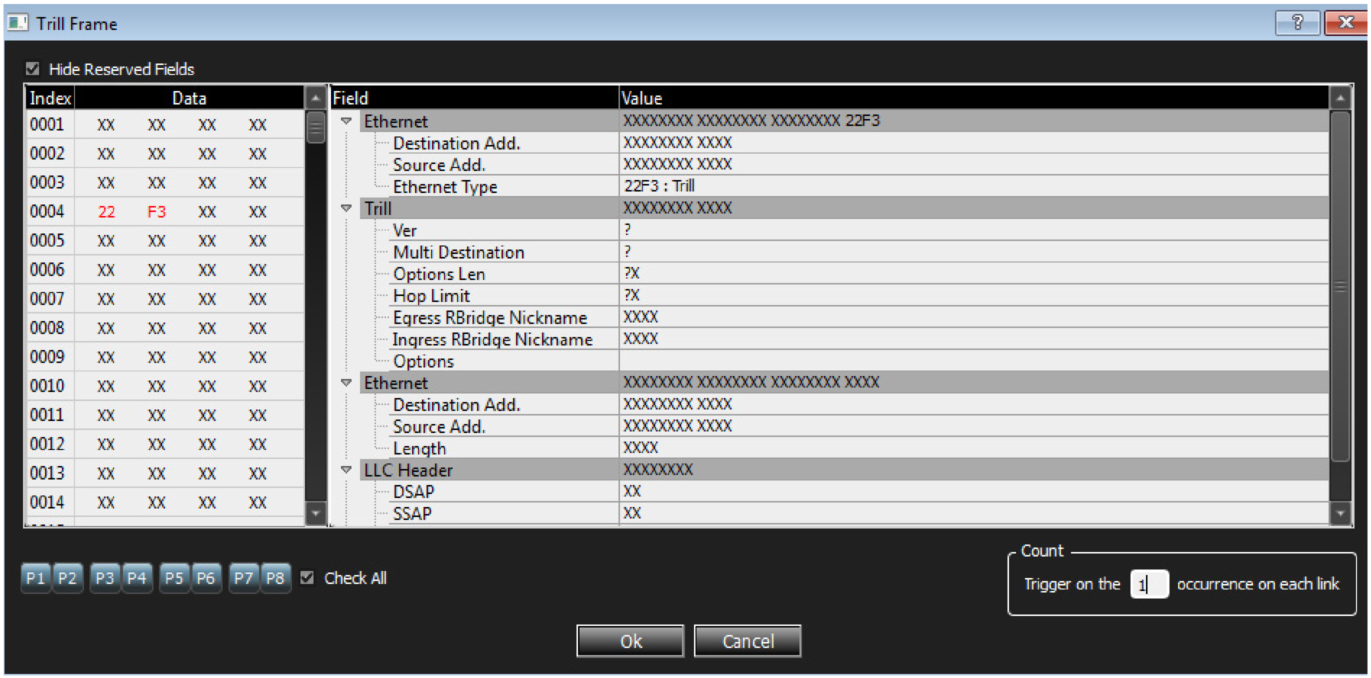
Trigger on the 1 occurrence on each link

Figure 2.67: IBXoE Frame Dialog

Enter the values for the Ethernet header, Global Routing Header (GRH), Base transport header (BTH) and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Trill Frame

Double-click **Trill Frame** to open the dialog.



Trill Frame

☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	22	F3	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX 22F3
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Ethernet Type	22F3 : Trill
Trill	XXXXXXXX XXXX
Ver	?
Multi Destination	?
Options Len	?X
Hop Limit	?X
Egress RBridge Nickname	XXXX
Ingress RBridge Nickname	XXXX
Options	
Ethernet	XXXXXXXX XXXXXXXX XXXXXXXX XXXX
Destination Add.	XXXXXXXX XXXX
Source Add.	XXXXXXXX XXXX
Length	XXXX
LLC Header	XXXXXXXX
DSAP	XX
SSAP	XX

P1 P2 P3 P4 P5 P6 P7 P8 ☑ Check All

Count

Trigger on the 1 occurrence on each link

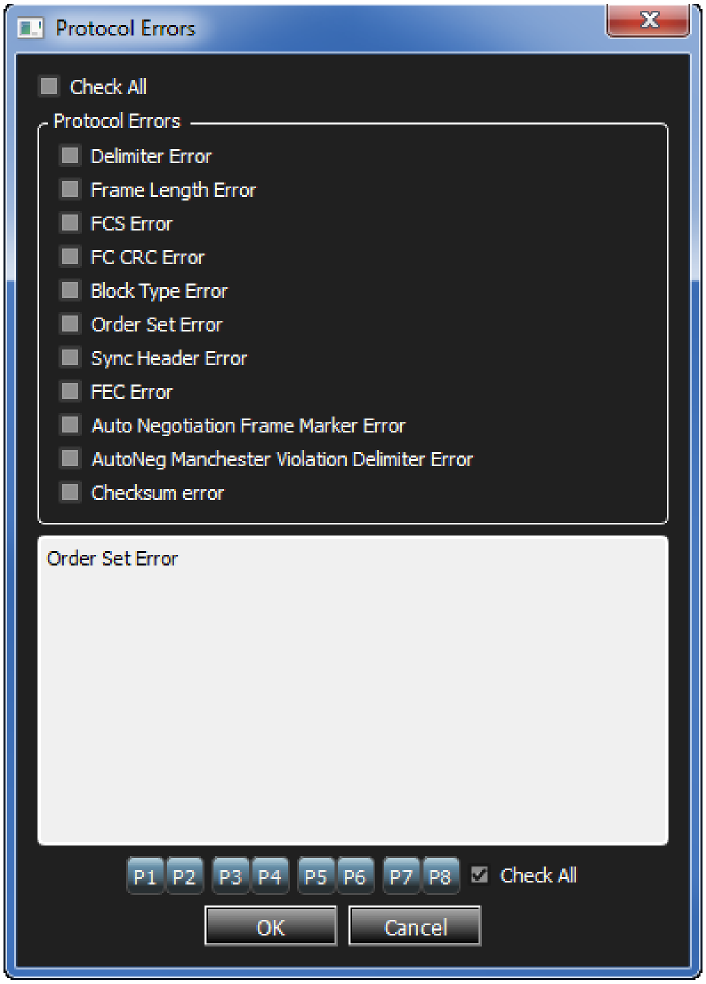
Ok Cancel

Figure 2.68: Trill Frame Dialog

Enter the values for the Ethernet header, Trill and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Protocol Errors

Double-click **Protocol Errors** to open the dialog.



□ Check All

Protocol Errors

□ Delimiter Error

□ Frame Length Error

□ FCS Error

□ FC CRC Error

□ Block Type Error

□ Order Set Error

□ Sync Header Error

□ FEC Error

□ Auto Negotiation Frame Marker Error

□ AutoNeg Manchester Violation Delimiter Error

□ Checksum error

Order Set Error

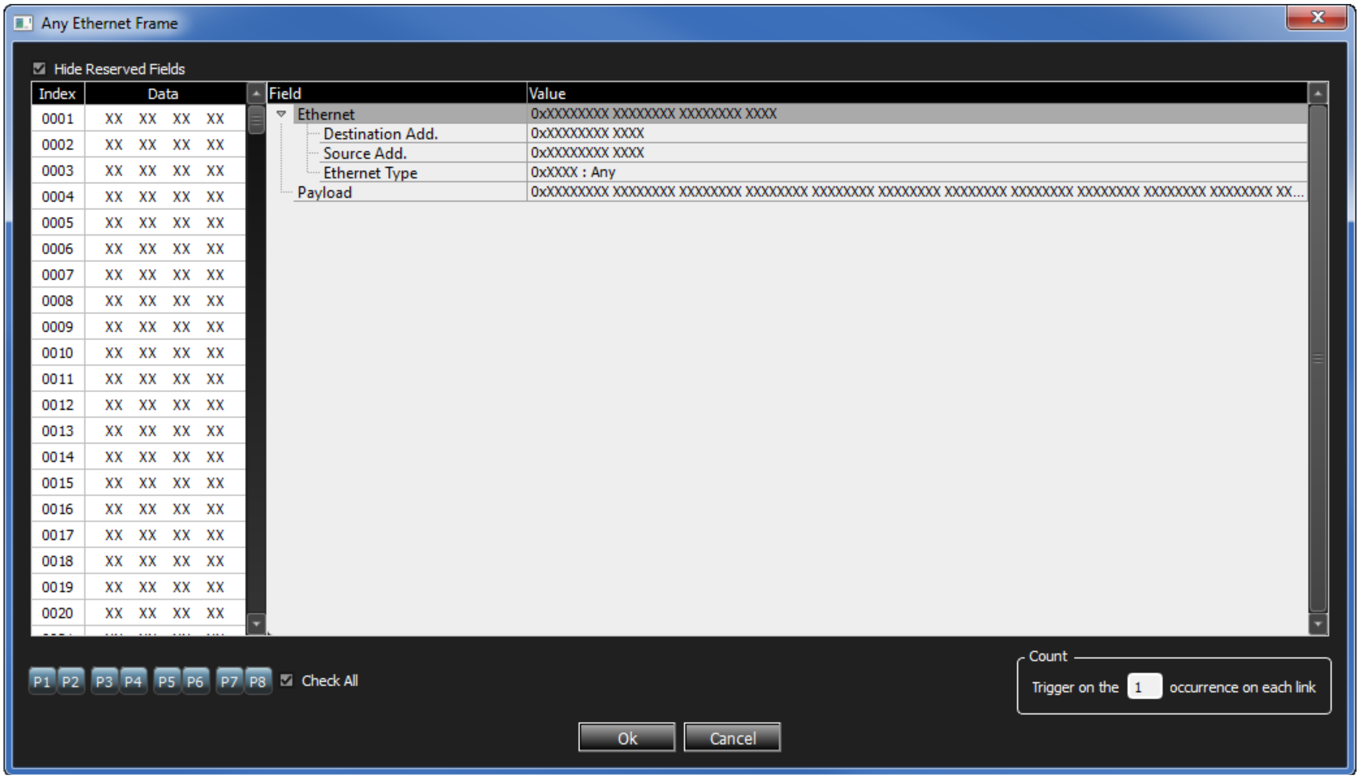
☑ Check All

Figure 2.69: Protocol Errors Dialog

Select the desired protocol errors or click on the **Check All** box to select all the errors. Enter the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Any Ethernet Frame

Double-click **Any Ethernet Frame** to open the dialog.



☑ Hide Reserved Fields

Index	Data
0001	XX XX XX XX
0002	XX XX XX XX
0003	XX XX XX XX
0004	XX XX XX XX
0005	XX XX XX XX
0006	XX XX XX XX
0007	XX XX XX XX
0008	XX XX XX XX
0009	XX XX XX XX
0010	XX XX XX XX
0011	XX XX XX XX
0012	XX XX XX XX
0013	XX XX XX XX
0014	XX XX XX XX
0015	XX XX XX XX
0016	XX XX XX XX
0017	XX XX XX XX
0018	XX XX XX XX
0019	XX XX XX XX
0020	XX XX XX XX

Field	Value
Ethernet	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXX
Destination Add.	0xXXXXXXXX XXXX
Source Add.	0xXXXXXXXX XXXX
Ethernet Type	0xXXXX : Any
Payload	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XX...

☑ Check All

Count

Trigger on the 1 occurrence on each link

Figure 2.70: Any Ethernet Frame Dialog

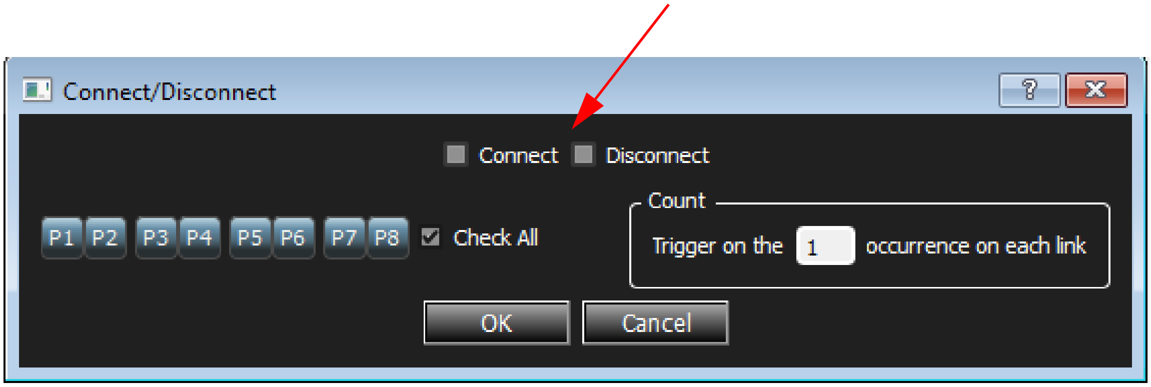
Enter the values for the Ether header and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

2.7.9 FC Patterns (Easy Mode)

Basic Patterns

Connect/Disconnect

Double-click **Connect/Disconnect** to open the **Connect/Disconnect** dialog.



□ Connect □ Disconnect

☑ Check All

Count

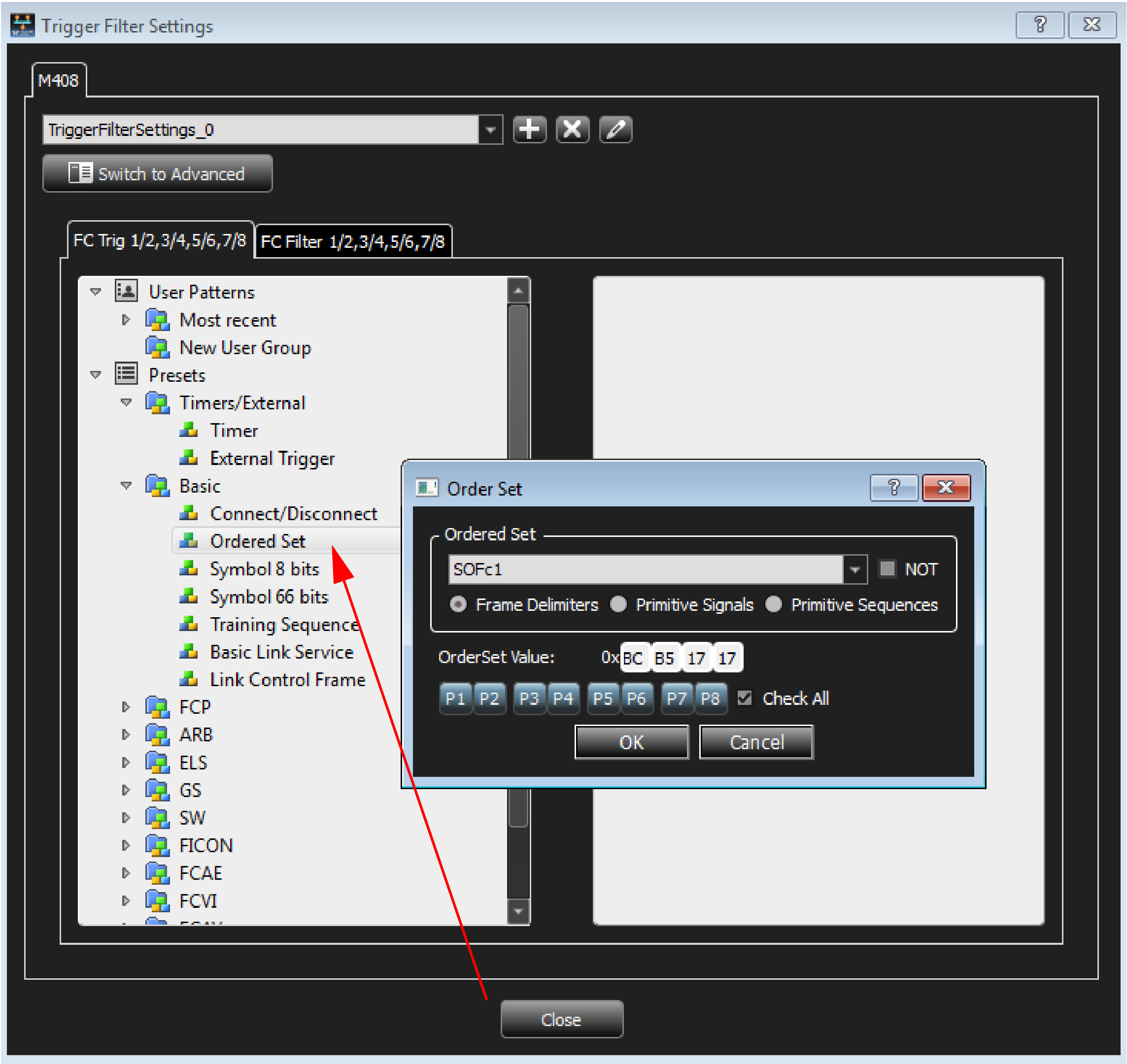
Trigger on the 1 occurrence on each link

Figure 2.71: Connect/Disconnect Dialog

Select **Connect/Disconnect** and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Ordered Set

Double-click **Ordered Set** to open the **Order Set** dialog.



TriggerFilterSettings_0

Ordered Set: SOFc1 □ NOT

● Frame Delimiters ○ Primitive Signals ○ Primitive Sequences

OrderSet Value: 0x BC B5 17 17

☑ Check All

Figure 2.72: Order Set Pattern Dialog

Select the values for the Ordered Set from the drop-down list. Select Frame Delimiters, Primitive Signals and Primitive Sequences as applicable. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Symbol 8 Bits

Double-click **Symbol 8 bits** to open the Symbol 8G Pattern dialog.

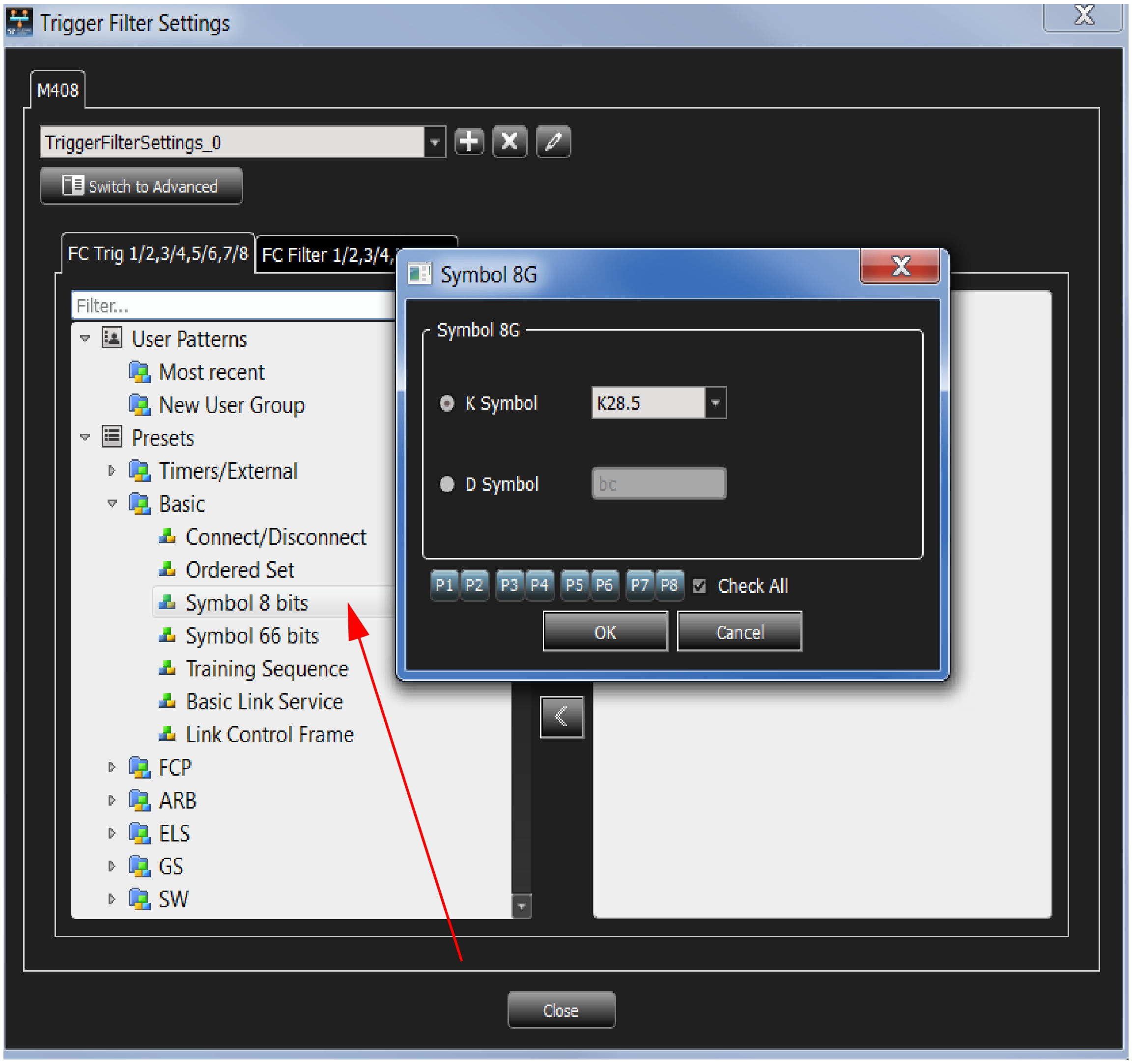
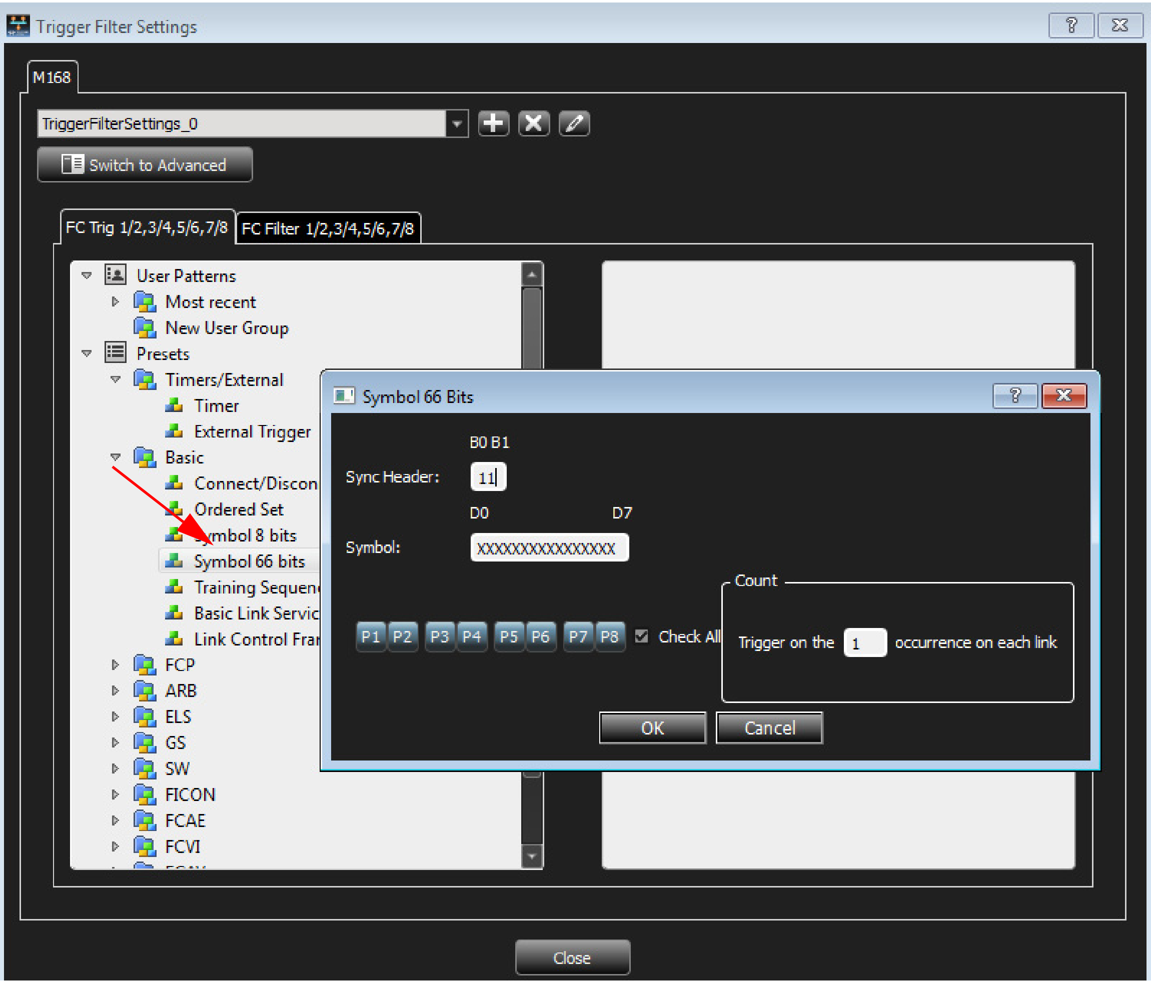


Figure 2.73: Symbol 8G Pattern Dialog

Check K Symbol or D Symbol as applicable. Select the value for K Symbol from the drop-down list or enter the value for D Symbol. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Symbol 66 Bits

Double-click **Symbol 66 bits** to open the Symbol 66 Bits Pattern dialog.



Sync Header: 11

Symbol: XXXXXXXXXXXXXXXX

☑ Check All

Trigger on the 1 occurrence on each link

Figure 2.74: Symbol 66 Bits Pattern Dialog

Enter the values for the Sync Header, Symbol and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

Two different order sets can exist in one 64 bits payload of a 66 bits block. The six examples of a remote and local fault given below demonstrate how to manually enter ordered set triggers.

0x0100000001000055 -> local fault-local fault

0x000000000100004b -> local fault-idle

0x010000000000002D -> idle-local fault

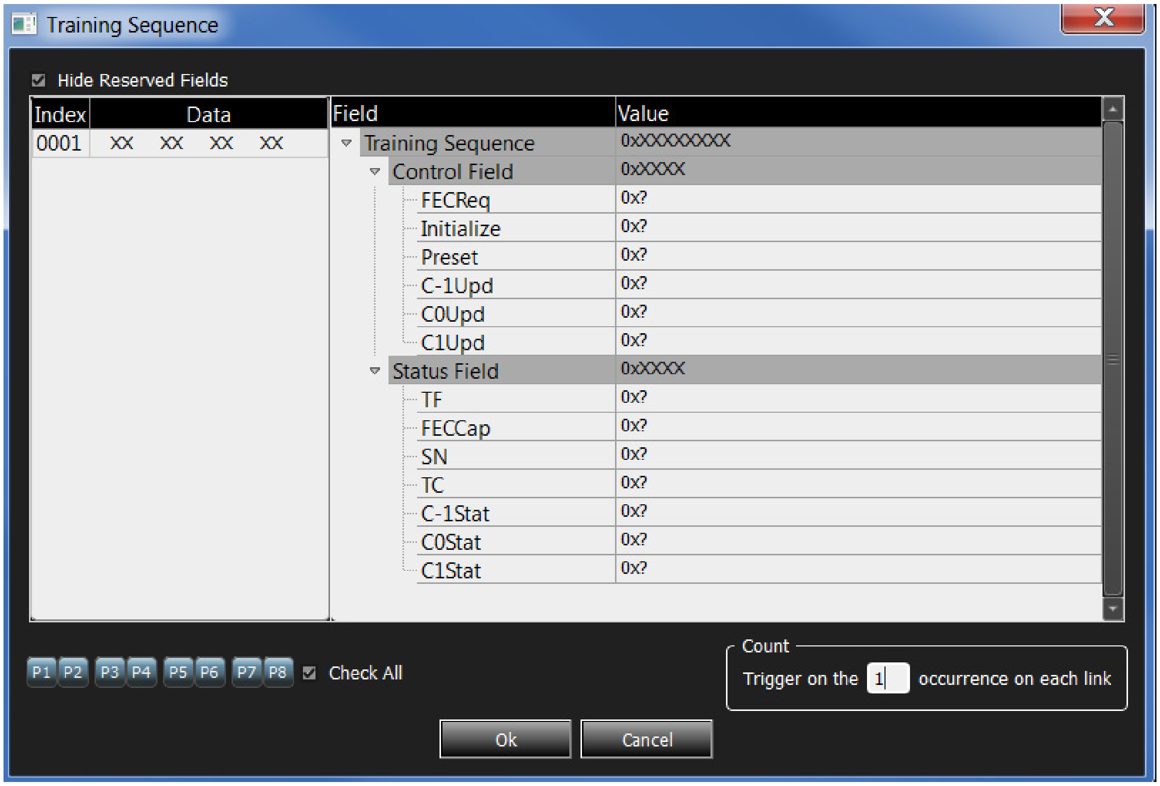
0x0200000002000055 -> remote fault-remote fault

0x000000000200004b -> remote fault-idle

0x020000000000002D -> idle-remote fault

Training Sequence

Double-click **Training Sequence** to open the Training Sequence dialog.



☑ Hide Reserved Fields

Index	Data
0001	XX XX XX XX

Field	Value
Training Sequence	0xXXXXXXXX
Control Field	0xXXXX
FECReq	0x?
Initialize	0x?
Preset	0x?
C-1Upd	0x?
C0Upd	0x?
C1Upd	0x?
Status Field	0xXXXX
TF	0x?
FECCap	0x?
SN	0x?
TC	0x?
C-1Stat	0x?
C0Stat	0x?
C1Stat	0x?

☑ Check All

Count

Trigger on the 1 occurrence on each link

Figure 2.75: Training Sequence Dialog

Enter the values for Control and Status Fields and the count of the expected number of occurrences.

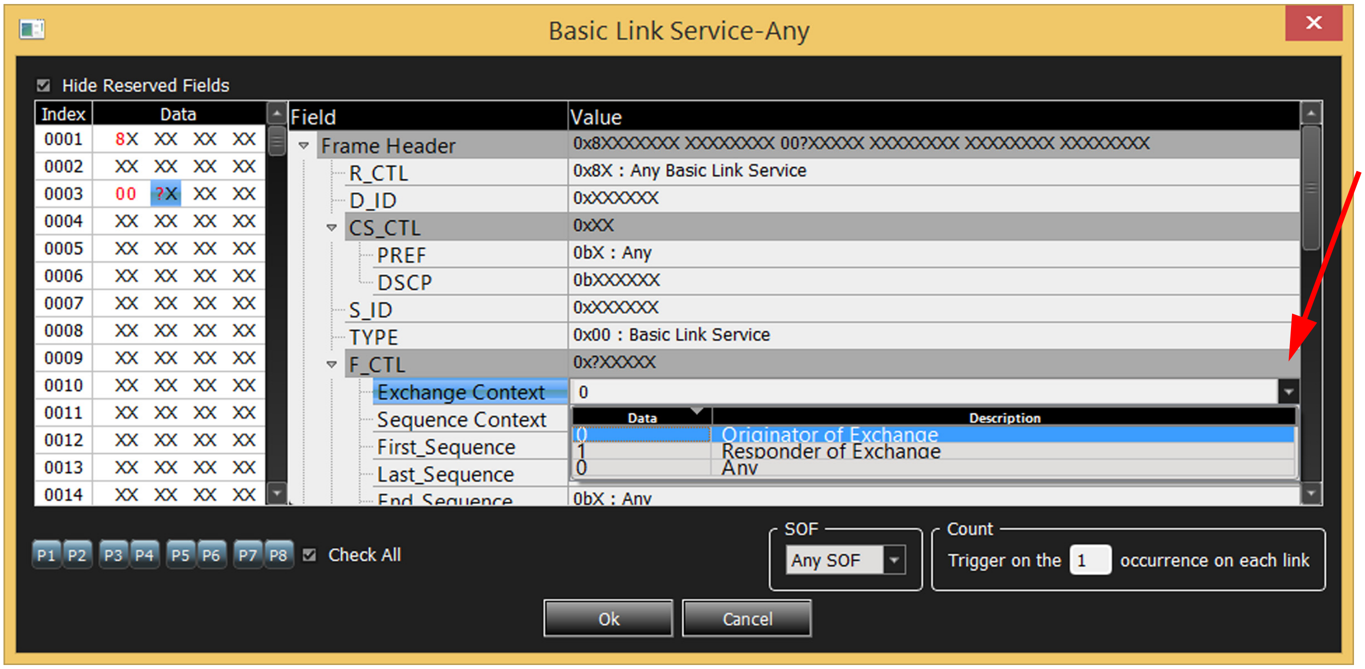
Check the **Check All** box to select ports P1 through P8 or individually select ports.

Basic Link Service

Double-click **Basic Link Service** to open the Basic Link Service Pattern dialog.

For any FC pattern, double-click the pattern name, for example, double-click **Basic Link Service** to open the Basic Link Service Pattern dialog.

Note: Some screen captures for the FC patterns are similar to the screen capture shown below.



Basic Link Service-Any

☑ Hide Reserved Fields

Index	Data			
0001	8X	XX	XX	XX
0002	XX	XX	XX	XX
0003	00	?X	XX	XX
0004	XX	XX	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Frame Header	0x8XXXXXXX XXXXXXXX 00?XXXXX XXXXXXXX XXXXXXXX XXXXXXXX
R_CTL	0x8X : Any Basic Link Service
D_ID	0xXXXXXX
CS_CTL	0xXX
PREF	0bX : Any
DSCP	0bXXXXXX
S_ID	0xXXXXXX
TYPE	0x00 : Basic Link Service
F_CTL	0x?XXXXX
Exchange Context	0
Sequence Context	
First_Sequence	
Last_Sequence	
End_Sequence	0bX : Any

Data	Description
0	Originator of Exchange
1	Responder of Exchange
0	Any

P1 P2 P3 P4 P5 P6 P7 P8 ☑ Check All

SOF: Any SOF

Count: Trigger on the 1 occurrence on each link

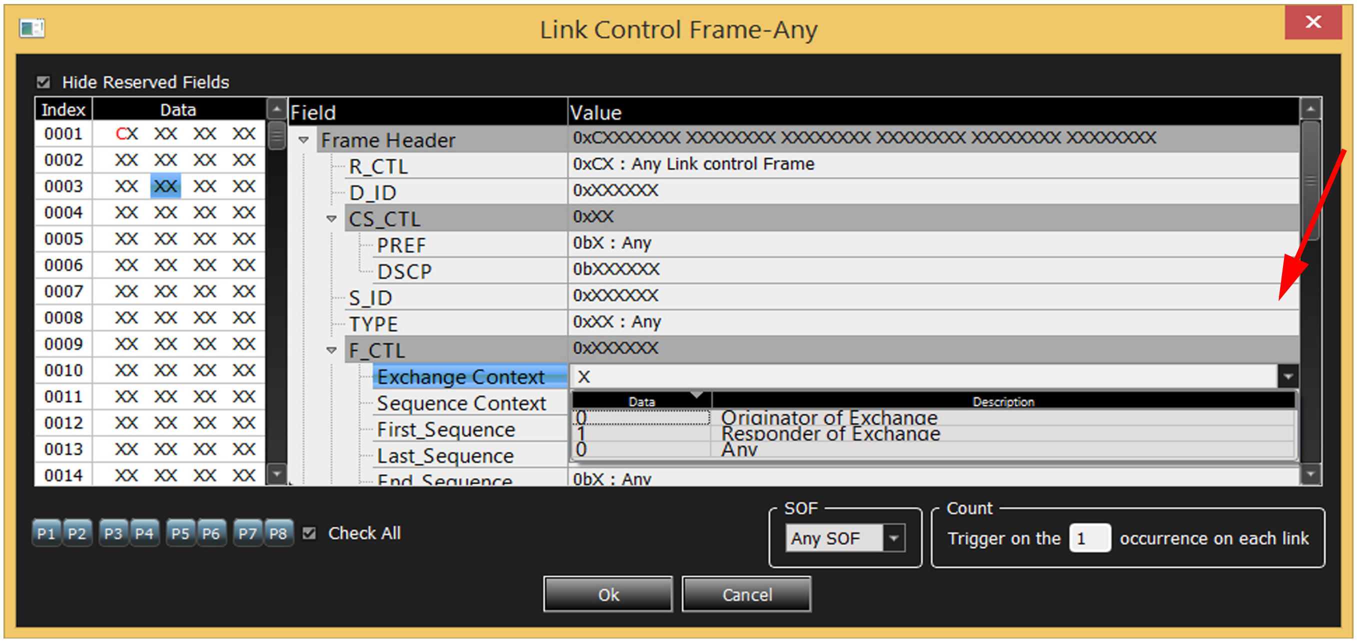
Figure 2.76: Basic Link Service Pattern Dialog

Enter the values for the Frame Header, CS_CTL, F_CTL and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports. You can specify the type of SOF to match on for the frame by selecting it from the SOF drop-down list.

Note: Some patterns have additional options to select from drop-drown lists as shown in the figure above.

Link Control Frame

Double-click **Link Control Frame** in the Pattern window to open the Add Link Control Frame Pattern dialog.



☑ Hide Reserved Fields

Index	Data			
0001	CX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	XX	XX	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

Field	Value
Frame Header	0xCXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
R_CTL	0xCX : Any Link control Frame
D_ID	0xXXXXXX
CS_CTL	0xXX
PREF	0bX : Any
DSCP	0bXXXXXX
S_ID	0xXXXXXX
TYPE	0xXX : Any
F_CTL	0xXXXXXX
Exchange Context	X
Sequence Context	
First_Sequence	
Last_Sequence	
End_Sequence	0bX : Any

Data	Description
0	Originator of Exchange
1	Responder of Exchange
0	Any

☑ Check All

SOF: Any SOF

Count: Trigger on the 1 occurrence on each link

Figure 2.77: Link Control Frame Pattern Dialog

Enter the values for the Frame Header, CS_CTL, F_CTL and the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P4 or individually select ports. You can specify the type of SOF to match on for the frame by selecting it from the SOF drop-down list.

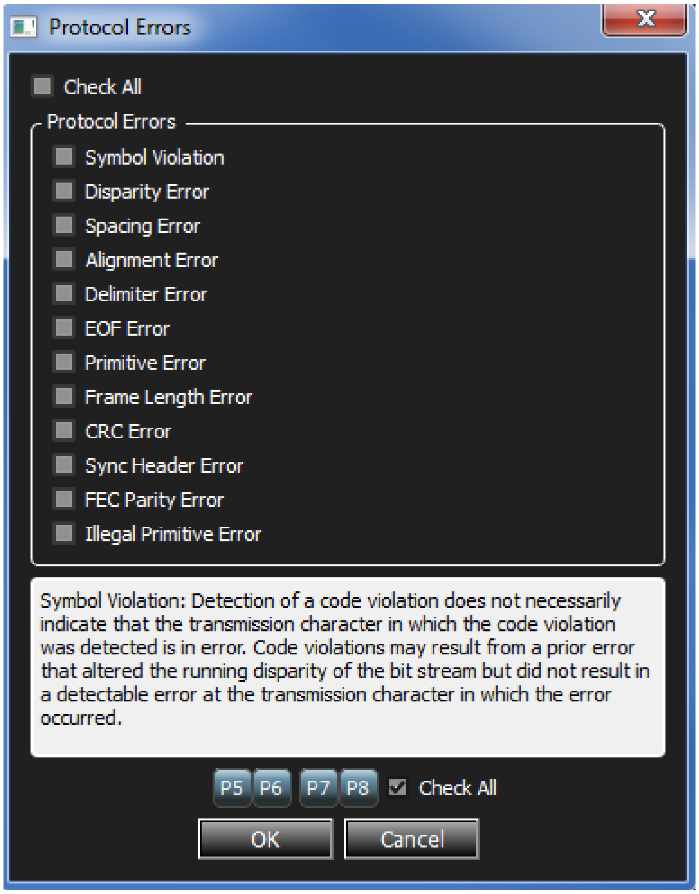
The following additional FC patterns are available:

Other FC Patterns

The same pattern types listed for FCoE are also available for native FC as well. Refer to "FCoE Patterns" on page 77 above.

FC Protocol Errors

Double-click **Protocol Errors** to open the dialog.



Protocol Errors

□ Check All

Protocol Errors

- □ Symbol Violation
- □ Disparity Error
- □ Spacing Error
- □ Alignment Error
- □ Delimiter Error
- □ EOF Error
- □ Primitive Error
- □ Frame Length Error
- □ CRC Error
- □ Sync Header Error
- □ FEC Parity Error
- □ Illegal Primitive Error

Symbol Violation: Detection of a code violation does not necessarily indicate that the transmission character in which the code violation was detected is in error. Code violations may result from a prior error that altered the running disparity of the bit stream but did not result in a detectable error at the transmission character in which the error occurred.

Figure 2.78: Protocol Errors Dialog

Select the desired protocol errors or click on the **Check All** box to select all the errors. Enter the count of the expected number of occurrences. Check the **Check All** box to select ports P1 through P8 or individually select ports.

2.7.10 Trigger Setup

You can specify when the analyzer triggers. Two trigger modes are available: The default mode is **Snapshot** or you can select **Event Trigger.**

When data capture starts with **Don't care (Snapshot)** selected, the analyzer triggers on the first data pattern on the bus.

Starting a data capture with **Pattern** selected triggers when specific pattern(s) are detected in the captured data stream. The following three ways can trigger the analyzer with **Pattern** selected:

- ❑ Trigger on any pattern (Any Trigger Mode)
- ❑ External Trigger
- ❑ Trigger on a sequence of patterns (Sequential Trigger Mode)

Snapshot Mode

To trigger immediately on any pattern, check the **Snapshot** button.

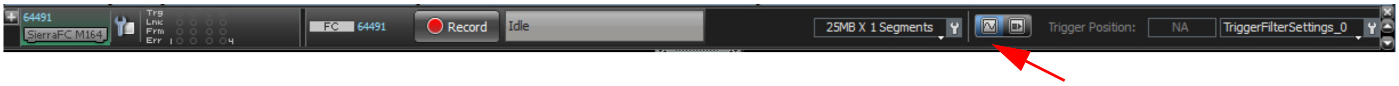


Figure 2.79: Default Trigger Snapshot Mode Selected

Manual Trigger

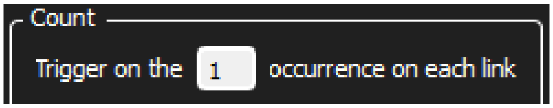
In the **Manual Trigger** mode, the analyzer captures bus traffic continually from when you use the Manual Trigger until you click the **Stop Hardware** button (on the analyzer toolbar), which triggers the analyzer.

Timer
See “Timer” on page 72 for more information.

Defining Patterns

The definition of patterns for the sequential trigger mode is identical to the Pattern mode, with the following exception:

In sequential triggering mode, all the pattern dialogs display the option for setting to count the expected number of occurrences on each link. This allows you to specify the number of times that the pattern must occur before triggering or proceeding in the trigger sequence.



Count

Trigger on the 1 occurrence on each link

Figure 2.80: Number of Occurrences

Note: The Events on each link are counted independently, causing a trigger whenever the number of occurrences on any link equals the specified value.

Pre-Trigger

You can set the amount of data to capture before and after the trigger, as a percentage of pre-trigger, between 0% and 100%. Position the pre-trigger slider to a percentage. This feature allows the evaluation of bus activity leading up to and after the triggering Event. Figure 2.81: illustrates the operation of pre-trigger in data memory.

Pre-trigger data is capture of the specified percentage of data prior to the triggering Event. It cannot be guaranteed and may be 0. This can occur when the triggering Event occurs before storing the required amount of pre-trigger Event data. In such a case, the data display shows fewer than the specified data points prior to the triggering Event.

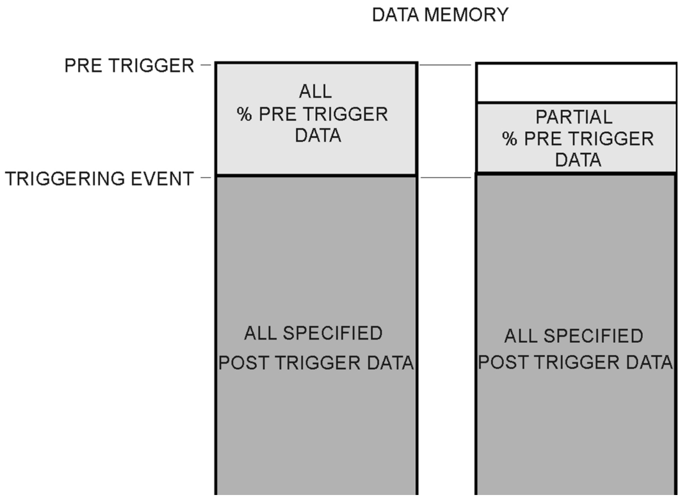


Figure 2.81: Pre-Trigger Example, 20% Pre-Trigger

Buffer Size and Segments

The Analyzer Settings panel has the Recording Buffer pane where you can set Number of Segments and the Segment Size. The defaults are one segment of 25MB. The total size used is automatically displayed for you. Setting multiple segments will allow to trigger on the first occurrence of the trigger condition, fill up the first segment, then automatically re-arm the trigger and repeat the remaining number of segments specified. You can use the slider button or click the up or down arrow to change memory usage for recording trace data. (Minimum size of memory is 1MB. Maximum size of memory is dependent on the hardware.) (See Figure 2.36 on page 59.) Enter an integer **Num. of Segment**, from 1 to 32, then enter an integer **Segment Size** in kilobytes, up to the memory size in megabytes divided by the number of segments. The default 1.

The New Project dialog opens with default settings to capture Everything on the bus and to Trigger On on Snapshot. (The analyzer captures everything immediately without triggering on anything in particular.)

Each time a trigger condition occurs, the system records a new segment. You can use a Snapshot or Pattern trigger, but not Manual Trigger. As the same trigger automatically repeats, the system makes the number of segments that you entered.

Note: If the size of a data packet exceeds the buffer memory allocation, the project runs, but no data capture occurs. You must increase buffer memory size to a value greater than the packet size.

Trigger Position

You can set the trigger position in the captured buffer as a percentage of the segment size. Trigger point of 0% means the trigger point will be on the first packet in the buffer.

To upload segments automatically for display as the system creates them, do not select the checkbox.This defaults to 1, which defines the amount of data to capture before and after the triggering Event. You can change this percentage by dragging the slider.

In certain cases, when one port is recording traffic and filling up the memory much faster than another port, you might see traffic appearing only on one port for a while, and the other port's traffic will only appear later. This occurs as a function of the trigger position, and is normal, expected behavior of the analyzer.

To upload segments manually in the Segment Manager, select the **Use upload manager (no automatic upload)** checkbox. To upload segments automatically for display as the system creates them, do not select the checkbox.

2.8 Advanced Mode (User-Defined)

Advanced Mode expands Analysis capability by allowing you to program complex triggering and data capture projects.

The Advanced Mode is a state machine. You can program each state individually to:

- Trigger on a different Event or trigger unconditionally.
- Capture Everything, Nothing, or a user-defined pattern.
- Include up to three ELSE IF statements, allowing a jump to any other state based on a user definition.
- Use up to three timers, which you can set to a maximum value of 4294900 ms or over one hour. If you enter a value larger than 42494900ms a warning pop-up displays: **Invalid value! Please enter a value between 0 and 4294900**.You can set a timer in the state or continue the timer set in the previous state.
- Output an external trigger High or Low.

Note: In Advanced Mode, Events on each link are counted independently. A condition is met if the number of Events on a link equals the defined occurrence.

2.8.1 Working in Advanced Mode

To start working in the Advanced Mode, click the **Switch to Advanced** mode button in the Trigger Filter Settings as shown in Figure 2.82.

You can:

- Display the state definition
- Set Output Trigger level
- Select up to three timers
- Define the If condition and up to three Else If conditions
- Set number of occurrences before trigger
- Set captured data
- Set excluded data
- Go to next state
- Add state
- Choose link for Sequencer setup

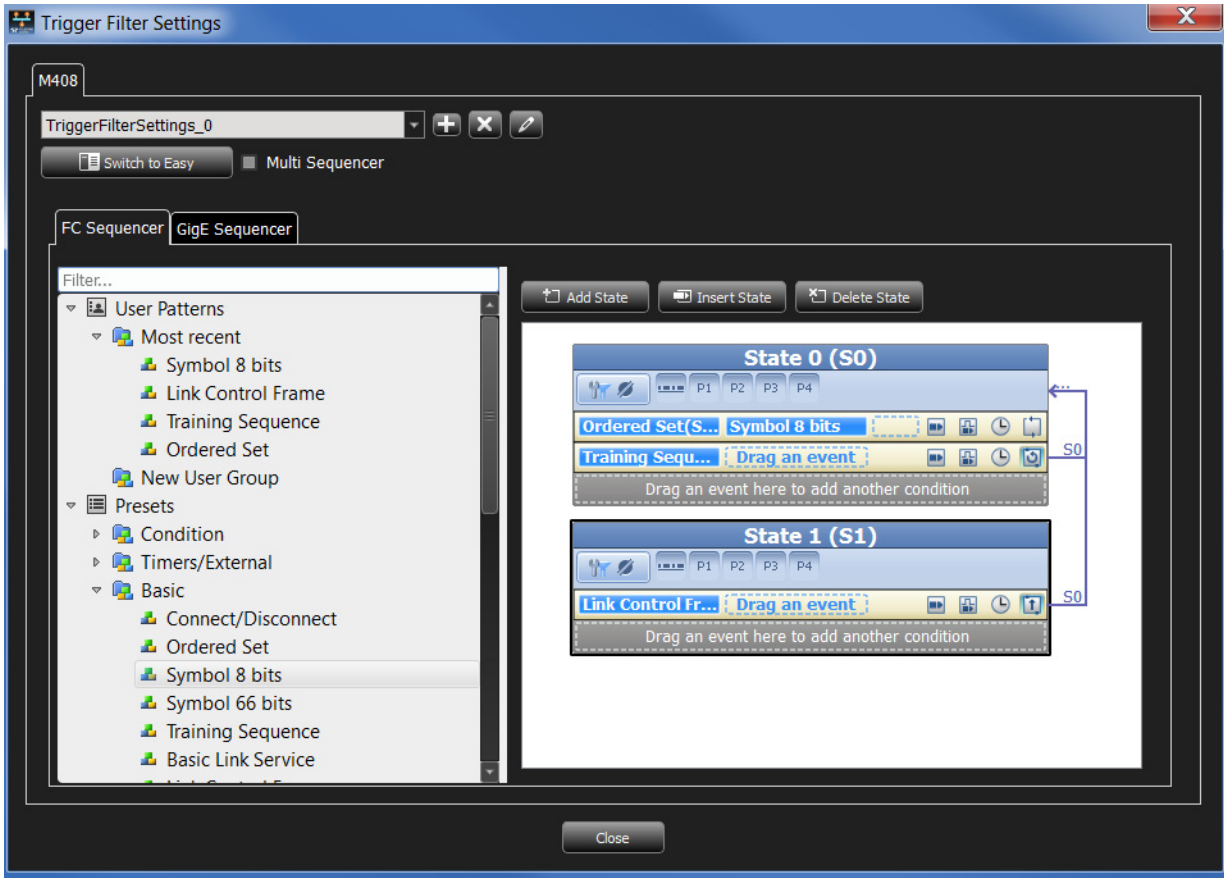


Figure 2.82: State Programming Dialog

Add State

Click on the Add State Add State button to add a State to the Sequencer. A State will be added below the last State.

Insert State

Select a State and click on the Insert State Insert State button to insert a State. A State will be inserted after a selected State.

Delete State

Select a State and click on the Delete State Delete State button to delete a State.

Copy/Cut and Paste States

You can copy and paste states within a Sequence.

1. Right-click in the blue title area of the State you want to copy and select Copy State (or Cut State if applicable).

2. Right-click in the white workspace of the desired target Sequence and select Paste State.

Copy/Cut and Paste Conditions

You can copy and paste Conditions within and between States.

1. Right-click in the empty yellow space of the Condition you want to copy and select Copy Condition (or Cut Condition if applicable).
2. Right-click in the gray placeholder area (i.e. in the area that says "Drag an event here....") of the desired target State and select Paste.

Copy/Cut and Paste Events

You can copy and paste Events within and between States.

1. Right-click on the Event you want to copy and select Copy (or Cut if applicable).
2. Right-click in the empty yellow space of the desired target Condition or in the gray placeholder area (i.e. in the area that says "Drag an event here....") of the desired target State and select Paste.

Adding Patterns to a State

1. Drag a pattern from the list of patterns displayed in the left panel and drop it in the State to add it. The application displays **Drag an event** or **Drag an event here to add another condition**, to indicate the location to drop events in a State. **Drag/Drop events** between states will copy/paste the event.
2. Define each selected pattern in the same way as in Easy Mode, as described in "Triggering/Filtering Patterns (Easy Mode)" on page 71. To use a timer, define it first.

Note: You can copy a frame from the spreadsheet view and paste it for triggering.

Note: You can set a timer for any If or Else If condition.

3. Enter a value for the number of occurrences before trigger in the **Count** field, up to a maximum of 65535 occurrences.

Setting Triggers

The trigger icon toggles between a blue outline and no outline, activating and deactivating it. Click the Trigger icon to activate the trigger. Once the trigger is activated the no outline trigger icon turns to blue outline.

External Output Trigger

The external output trigger icon toggles between a blue outline and no outline, activating and deactivating it. The External Output Trigger icon (no outline) indicates there is no change. Click to activate the trigger. Once the trigger is activated the icon has a blue outline indicating it is active.

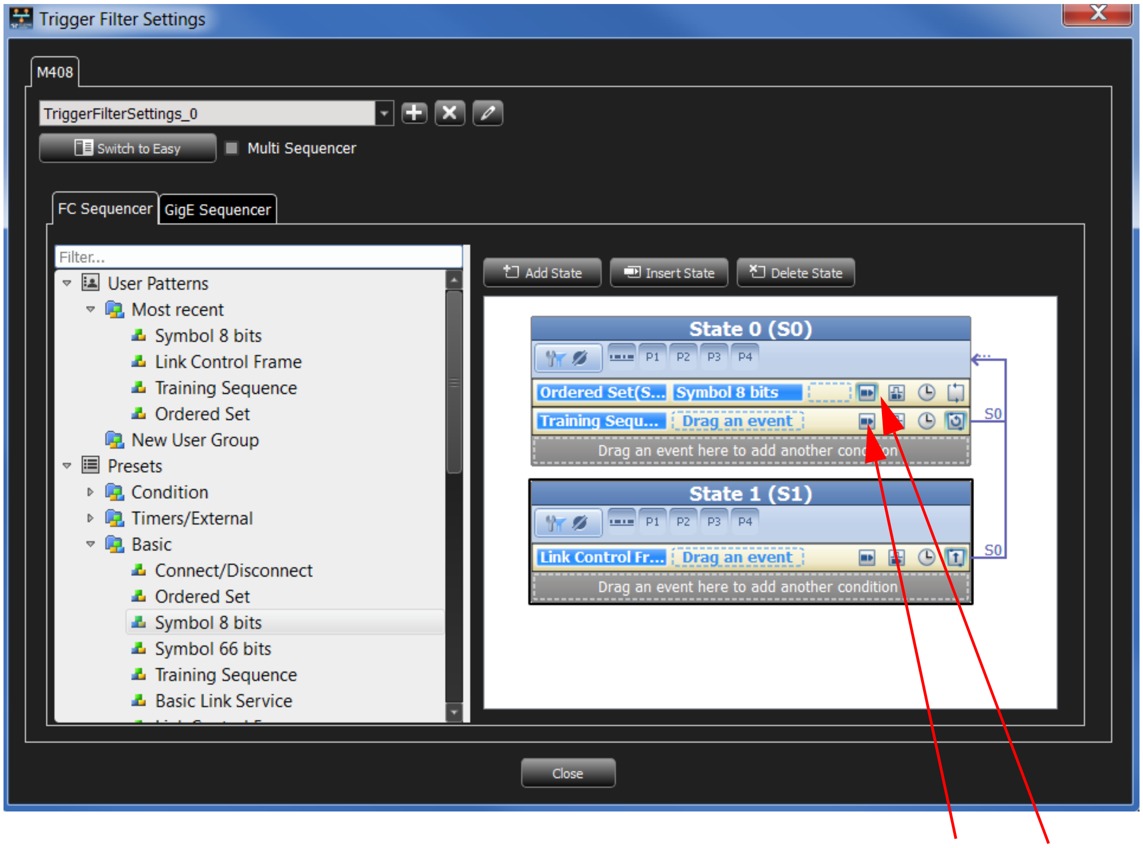


Figure 2.83: Setting Triggers

Setting State Transitions

Click on the State Transition icon to change the state to transition to. Left-click for menu options to display as shown in the following screen capture and select the state to transition to. To remove the state transition select **No Jump.**

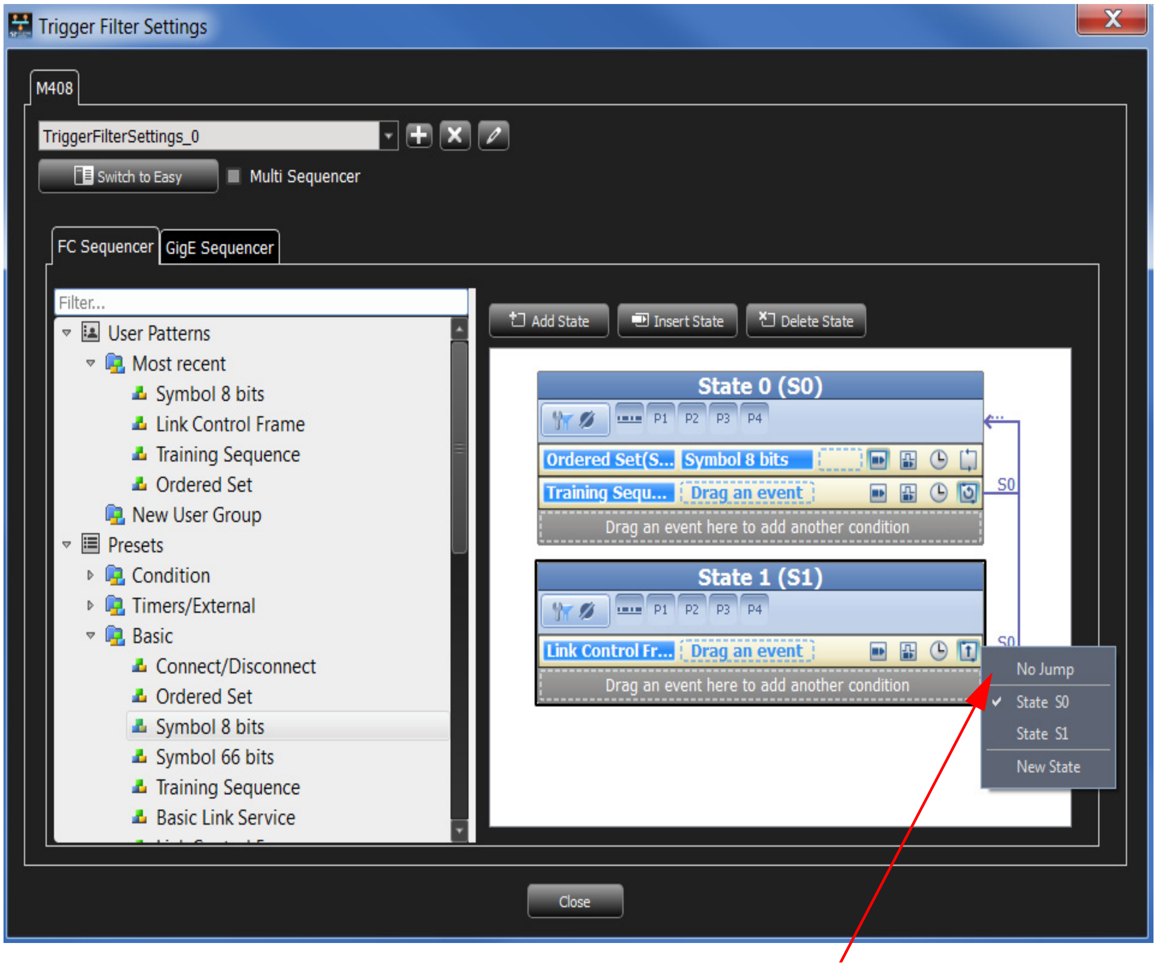


Figure 2.84: State Transition

Settings Capture Filters

- ❑ Choose a capture option by clicking on the Capture Everything icon shown in the figure below. The Filter Settings dialog displays (see Figure 2.86 on page 110.)

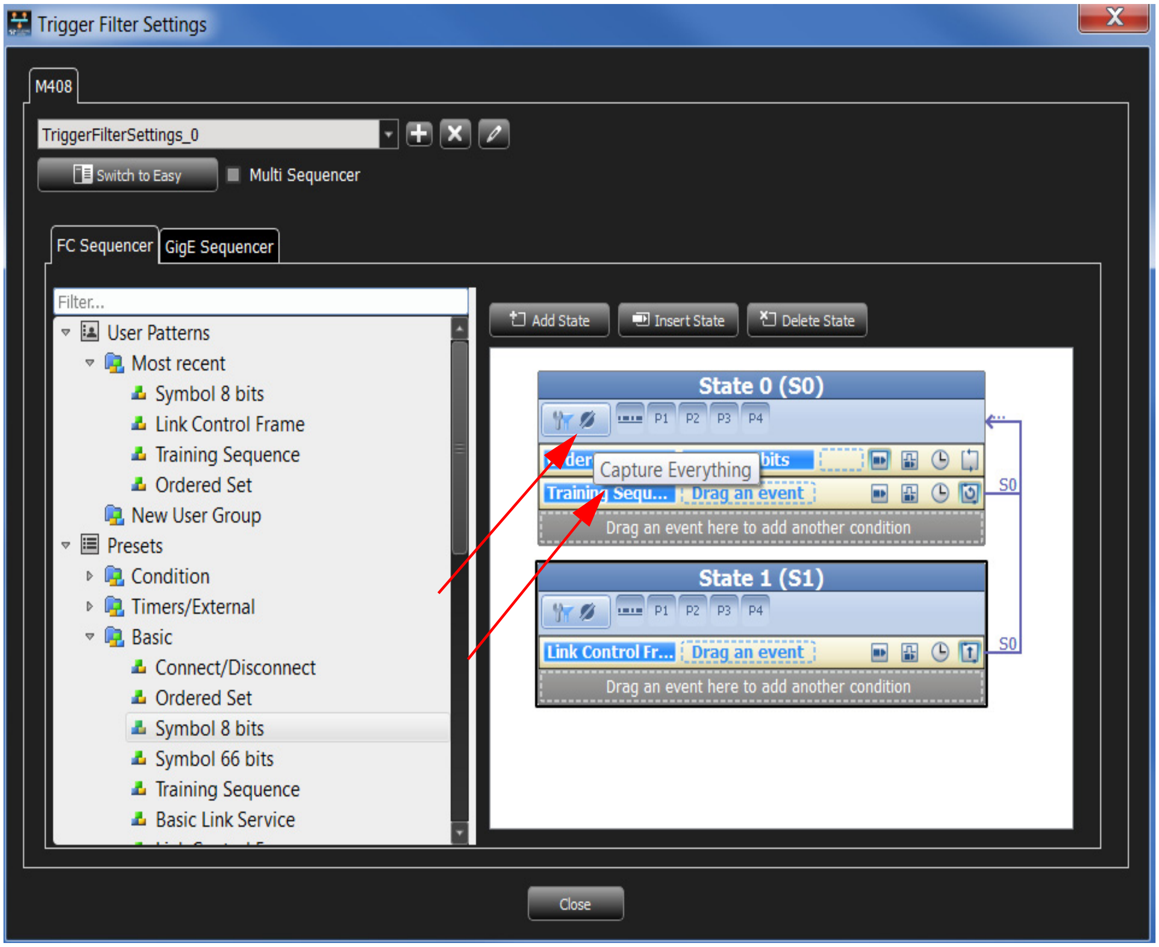


Figure 2.85: Capture Everything

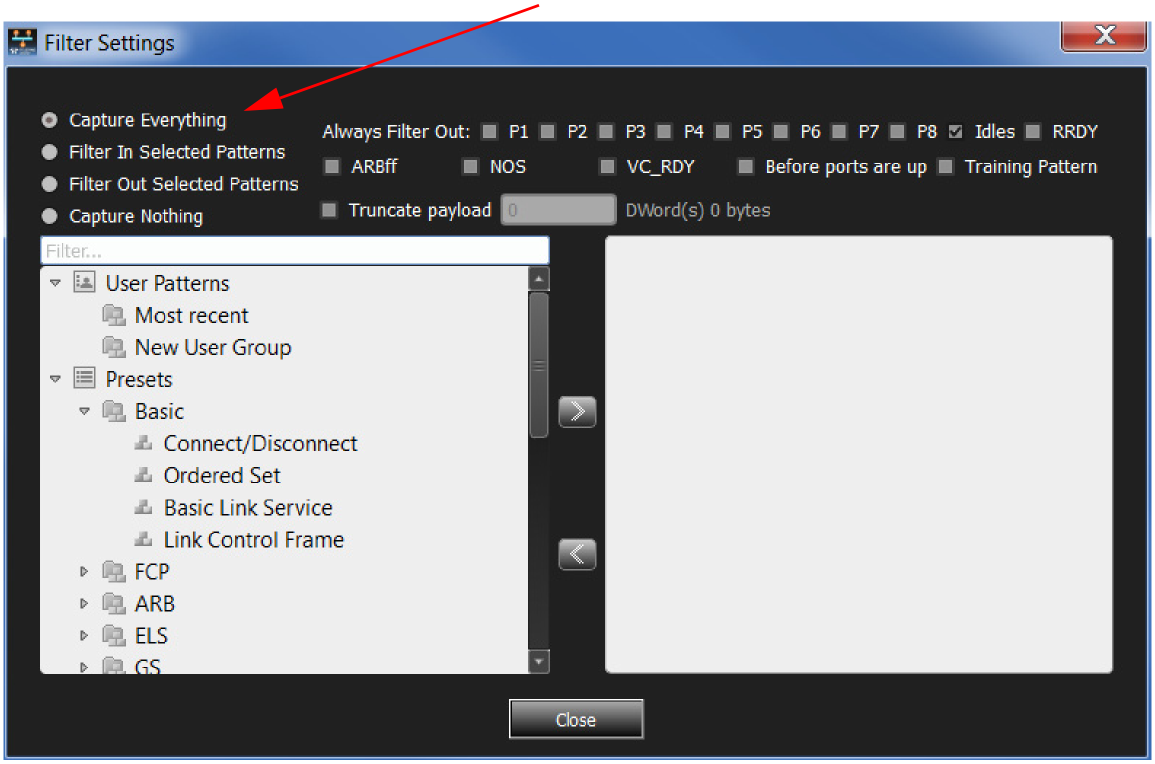

Filter Settings
X
● Capture Everything
● Filter In Selected Patterns
● Filter Out Selected Patterns
● Capture Nothing
Always Filter Out: □ P1 □ P2 □ P3 □ P4 □ P5 □ P6 □ P7 □ P8 ☑ Idles □ RRDY
□ ARBff □ NOS □ VC_RDY □ Before ports are up □ Training Pattern
□ Truncate payload 0 DWord(s) 0 bytes
Filter...
User Patterns
Most recent
New User Group
Presets
Basic
Connect/Disconnect
Ordered Set
Basic Link Service
Link Control Frame
FCP
ARB
ELS
GS
>
<
Close

Figure 2.86: Filter Settings Dialog

- If you choose Capture Everything, you can select Idles for exclusion.
- Select Filter In Selected Patterns or Filter Out Selected Patterns to select patterns for inclusion or exclusion (see Figure 2.86). See "Triggering/Filtering Patterns (Easy Mode)" on page 71.
- Choose pattern(s) and click the > button to add them for capture or exclusion. You define each pattern the same way as in Easy mode ("Triggering/Filtering Patterns (Easy Mode)" on page 71).
- Click Capture Nothing to run the trace without capturing anything.
- Click on the checkboxes to Always Filter Out Idles, RRDY or ports 1 through 8.
- Select ARBFF, NOS, VC_RDY, Before ports are up, or Training Pattern. ARBff, NOS and VC_RDY are ordered sets that show up frequently and are of little use in most cases, and selecting allows you to specifically filter them out. Before ports are up will filter everything before the ports are up, to save buffer space and allow to concentrate on the parts important to the user. Training Pattern will similarly filter out all Training Patterns
- Check the Truncate Payload option to truncate payload after x-number of Dword(s) 0 bytes. (see Figure 2.86).

Multi-Link Triggering

You can set different triggering for each link. To set different trigger conditions for a link, check the **Multi Sequencer** checkbox and select the link for setup from the Port tabs. When you select this option, you can define a sequencer per link (pair port). These sequencers are independent from each other and will be run separately on each link.

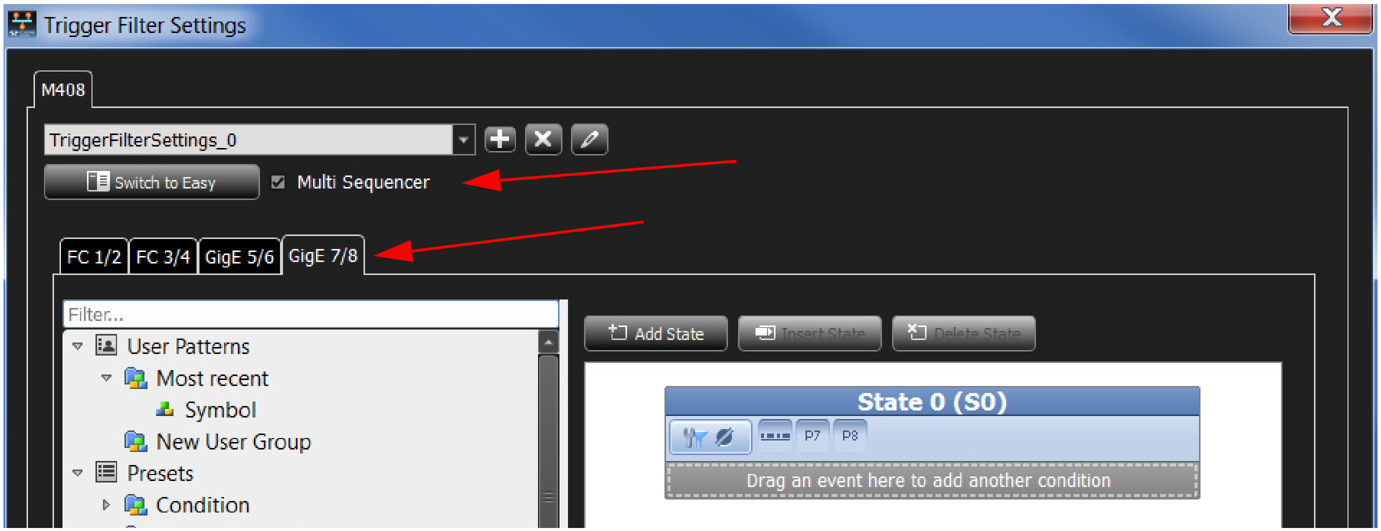
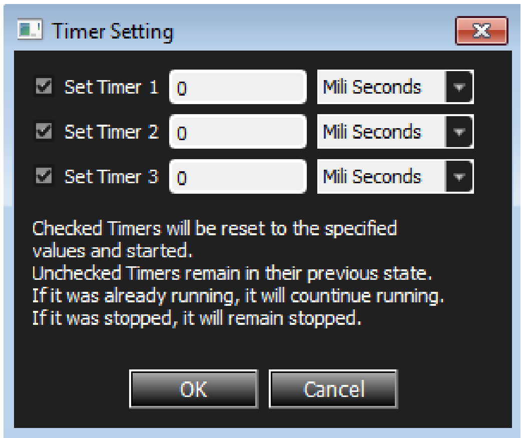


Figure 2.87: Multi-Link Triggering Setup

Set Timers

You can set and use up to three timers for triggering. You can set each timer for each state or continue from a timer set in the previous state. The timer defined for a particular state starts when entering that state. To set timers, click the Timer 🕒 icon in each state and define each of the timers in the Timer Setting dialog.


Timer Setting

☑ Set Timer 1 | 0 | Mili Seconds
☑ Set Timer 2 | 0 | Mili Seconds
☑ Set Timer 3 | 0 | Mili Seconds

Checked Timers will be reset to the specified values and started.
Unchecked Timers remain in their previous state.
If it was already running, it will countinue running.
If it was stopped, it will remain stopped.

Figure 2.88: Timer Settings Dialog

Three timers are available. You have to set and start each timer in order to continue the next timer. For example, you have to start Timer 1, continue it, then set Timer 2 in order to continue it. It will not allow you to continue Timer 2 until you first set it.

Chapter 3

Display Manipulation

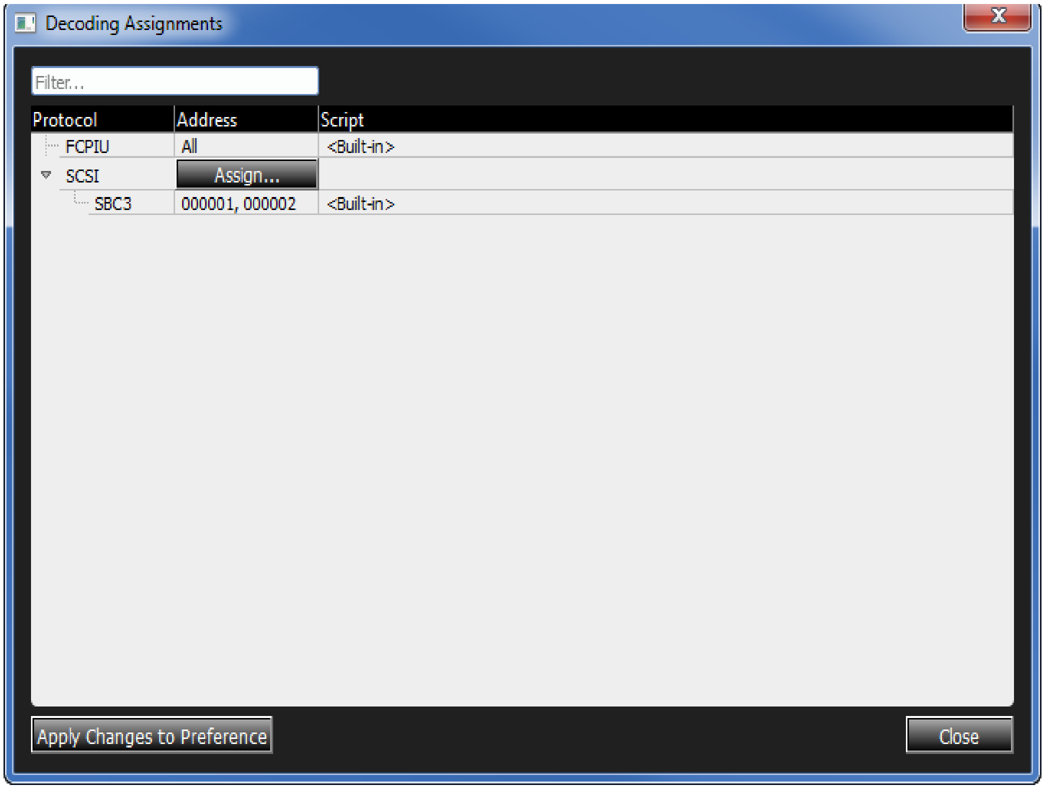
3.1 Viewer Display

After data is captured (Recorded), the Viewer displays the captured data and saves it as a trace file with a .get file extension.

Note that statistics are available only after the whole trace has uploaded. The data is available for analysis in various views which are explained in this section.

Click on **Analysis** in the Analyzer main menu options to enable and disable different trace views.

You can set decoding assignments by selecting **Analysis > Decoding Assignments...** The following Decoding Assignments dialog displays. For additional information see “Decoding Assignments” on page 117.

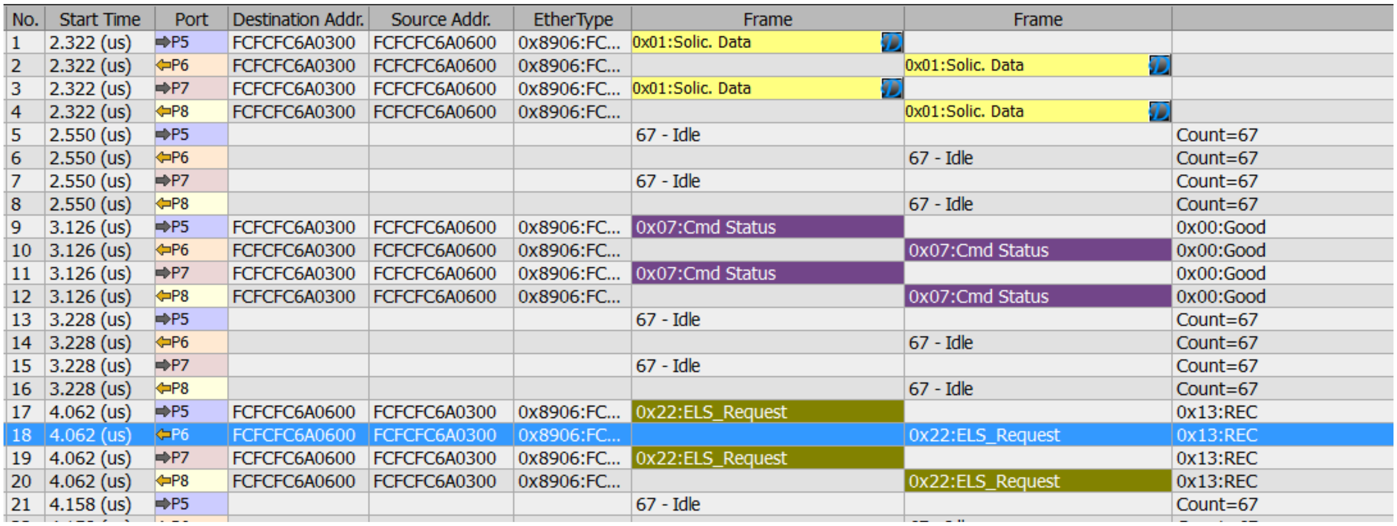


Protocol	Address	Script
FCPIU	All	<Built-in>
SCSI	Assign...	
SBC3	000001, 000002	<Built-in>

Figure 3.1: Decoding Assignments.

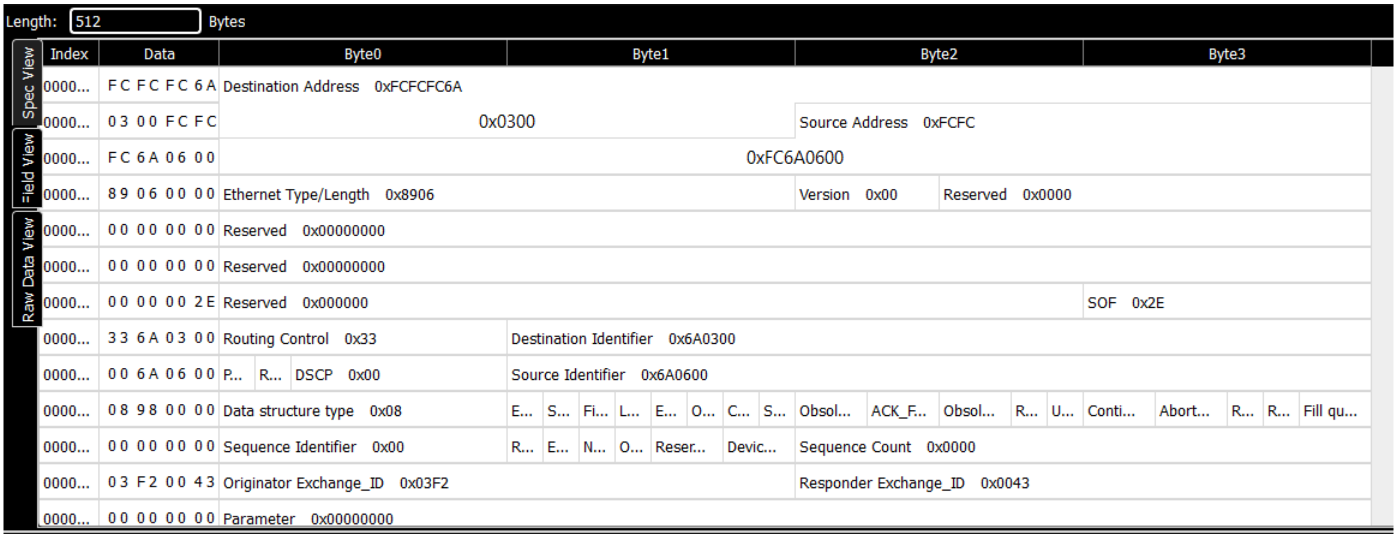
The following views are available for analysis (refer to the following screen captures):

- ❑ Spreadsheet View
- ❑ Frame Inspector
- ❑ Traffic Summary
- ❑ Data View



No.	Start Time	Port	Destination Addr.	Source Addr.	EtherType	Frame	Frame	
1	2.322 (us)	⇒P5	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x01:Solic. Data		
2	2.322 (us)	⇐P6	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x01:Solic. Data	
3	2.322 (us)	⇒P7	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x01:Solic. Data		
4	2.322 (us)	⇐P8	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x01:Solic. Data	
5	2.550 (us)	⇒P5				67 - Idle		Count=67
6	2.550 (us)	⇐P6					67 - Idle	Count=67
7	2.550 (us)	⇒P7				67 - Idle		Count=67
8	2.550 (us)	⇐P8					67 - Idle	Count=67
9	3.126 (us)	⇒P5	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x07:Cmd Status		0x00:Good
10	3.126 (us)	⇐P6	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x07:Cmd Status	0x00:Good
11	3.126 (us)	⇒P7	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...	0x07:Cmd Status		0x00:Good
12	3.126 (us)	⇐P8	FCFCFC6A0300	FCFCFC6A0600	0x8906:FC...		0x07:Cmd Status	0x00:Good
13	3.228 (us)	⇒P5				67 - Idle		Count=67
14	3.228 (us)	⇐P6					67 - Idle	Count=67
15	3.228 (us)	⇒P7				67 - Idle		Count=67
16	3.228 (us)	⇐P8					67 - Idle	Count=67
17	4.062 (us)	⇒P5	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...	0x22:ELS_Request		0x13:REC
18	4.062 (us)	⇐P6	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...		0x22:ELS_Request	0x13:REC
19	4.062 (us)	⇒P7	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...	0x22:ELS_Request		0x13:REC
20	4.062 (us)	⇐P8	FCFCFC6A0600	FCFCFC6A0300	0x8906:FC...		0x22:ELS_Request	0x13:REC
21	4.158 (us)	⇒P5				67 - Idle		Count=67

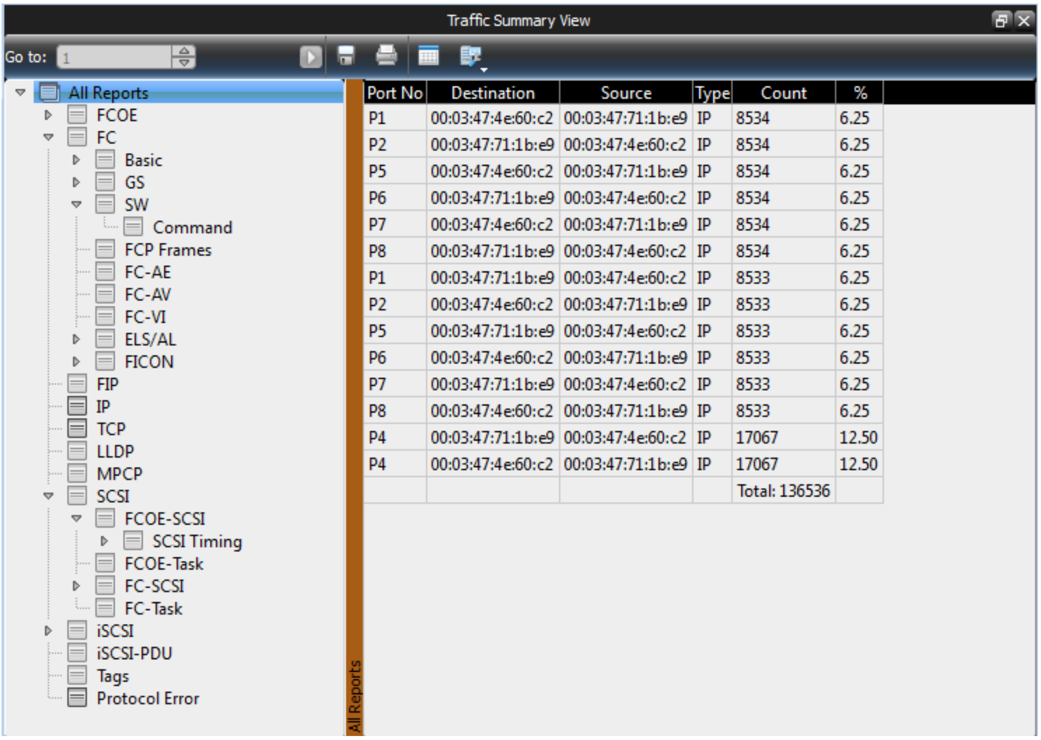
Figure 3.2: Spreadsheet View.



Length: 512 Bytes

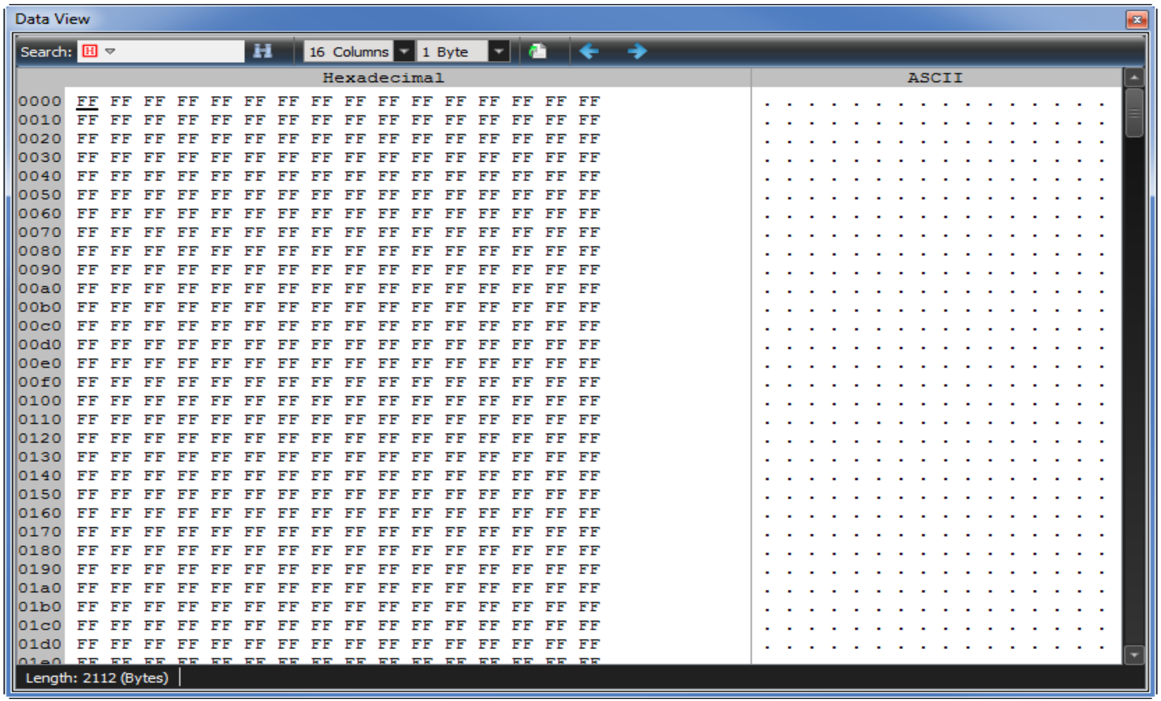
Index	Data	Byte0	Byte1	Byte2	Byte3
0000...	FC FC FC 6A	Destination Address 0xFCFCFC6A			
0000...	03 00 FC FC	0x0300		Source Address 0xFCFC	
0000...	FC 6A 06 00	0xFC6A0600			
0000...	89 06 00 00	Ethernet Type/Length 0x8906		Version 0x00 Reserved 0x0000	
0000...	00 00 00 00	Reserved 0x00000000			
0000...	00 00 00 00	Reserved 0x00000000			
0000...	00 00 00 2E	Reserved 0x000000			SOF 0x2E
0000...	33 6A 03 00	Routing Control 0x33	Destination Identifier 0x6A0300		
0000...	00 6A 06 00	P... R... DSCP 0x00	Source Identifier 0x6A0600		
0000...	08 98 00 00	Data structure type 0x08	E... S... Fi... L... E... O... C... S...	Obsol... ACK_F... Obsol... R... U...	Conti... Abort... R... R... Fill qu...
0000...	00 00 00 00	Sequence Identifier 0x00	R... E... N... O... Reser... Devic...	Sequence Count 0x0000	
0000...	03 F2 00 43	Originator Exchange_ID 0x03F2		Responder Exchange_ID 0x0043	
0000...	00 00 00 00	Parameter 0x00000000			

Figure 3.3: Frame Inspector View.



Port No	Destination	Source	Type	Count	%
P1	00:03:47:4e:60:c2	00:03:47:71:1b:e9	IP	8534	6.25
P2	00:03:47:71:1b:e9	00:03:47:4e:60:c2	IP	8534	6.25
P5	00:03:47:4e:60:c2	00:03:47:71:1b:e9	IP	8534	6.25
P6	00:03:47:71:1b:e9	00:03:47:4e:60:c2	IP	8534	6.25
P7	00:03:47:4e:60:c2	00:03:47:71:1b:e9	IP	8534	6.25
P8	00:03:47:71:1b:e9	00:03:47:4e:60:c2	IP	8534	6.25
P1	00:03:47:71:1b:e9	00:03:47:4e:60:c2	IP	8533	6.25
P2	00:03:47:4e:60:c2	00:03:47:71:1b:e9	IP	8533	6.25
P5	00:03:47:71:1b:e9	00:03:47:4e:60:c2	IP	8533	6.25
P6	00:03:47:4e:60:c2	00:03:47:71:1b:e9	IP	8533	6.25
P7	00:03:47:71:1b:e9	00:03:47:4e:60:c2	IP	8533	6.25
P8	00:03:47:4e:60:c2	00:03:47:71:1b:e9	IP	8533	6.25
P4	00:03:47:71:1b:e9	00:03:47:4e:60:c2	IP	17067	12.50
P4	00:03:47:4e:60:c2	00:03:47:71:1b:e9	IP	17067	12.50
				Total: 136536	

Figure 3.4: Traffic Summary View.



```
0000  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0010  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0020  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0030  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0040  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0050  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0060  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0070  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0080  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
00a0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
00b0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
00c0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
00d0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
00e0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
00f0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0100  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0110  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0130  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0140  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0150  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0160  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0170  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0180  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
0190  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
01a0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
01b0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
01c0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
01d0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF    ................
01e0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
Length: 2112 (Bytes)
```

Figure 3.5: Data View.

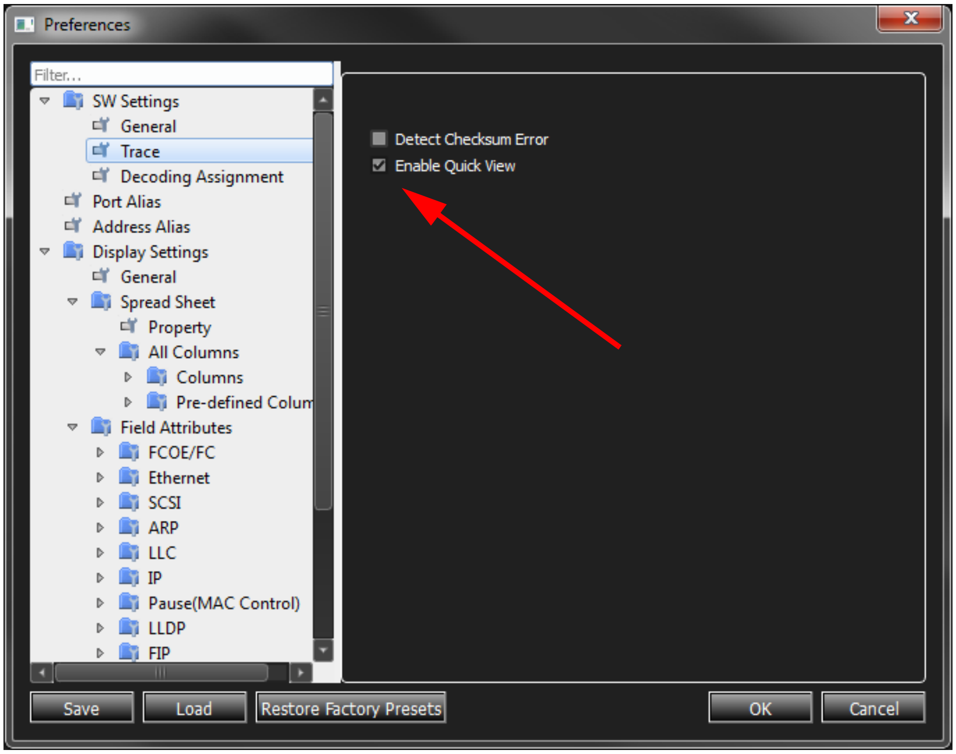
Note: You can change the colors of captured patterns of by selecting options in the **Preferences** > **Software Settings > Types** dialog.

3.2 Quick View

By default, the Software Settings enable **Quick View**. Quick View allows full access to the whole trace more quickly, especially when using a Gigabit Ethernet connection. However, the trace is NOT written to the host machine hard drive. To save the trace, you must manually select Save or Save As.

- If you select **Save**, the application saves the entire trace to a default file name. The trace remains open and its name is updated to reflect the saved location.
- If you select **Save As**, the application saves the trace to the specified location, and opens that trace from the new location. The original Quick View mode trace remains open as well.

If you de-select Quick View in the Software Settings to disable Quick View, then the trace loads more slowly, but is automatically saved to the host machine hard drive. When Quick View is enabled, the Viewer displays successive parts of trace data as they upload. As soon as a trace part uploads, it is available in all trace views.



□ Detect Checksum Error
☑ Enable Quick View

Figure 3.6: Enable Quick View

If you only need quick successive traces, and do not need to save them, keep the default setting to enable Quick View.

If you need to save all captured traces, de-selecting the Quick View setting loads the traces faster, especially for larger traces and slower connections.

To refresh the viewer display with more uploaded data, scroll to the end of the trace, using scroll bars, page down, arrow down, or CTRL-End. Newly uploaded data then appears there.

Note: High-level decoding and statistics are available only after the whole trace has uploaded.

After the trace finishes uploading, the software automatically switches to full trace view.

To go to the beginning of an uploaded trace, press CTRL Home, or CTRL End to go to the end of an uploaded trace.

3.3 Switching Views

To enable and disable views, use the Analysis menu item or the Analysis toolbar.

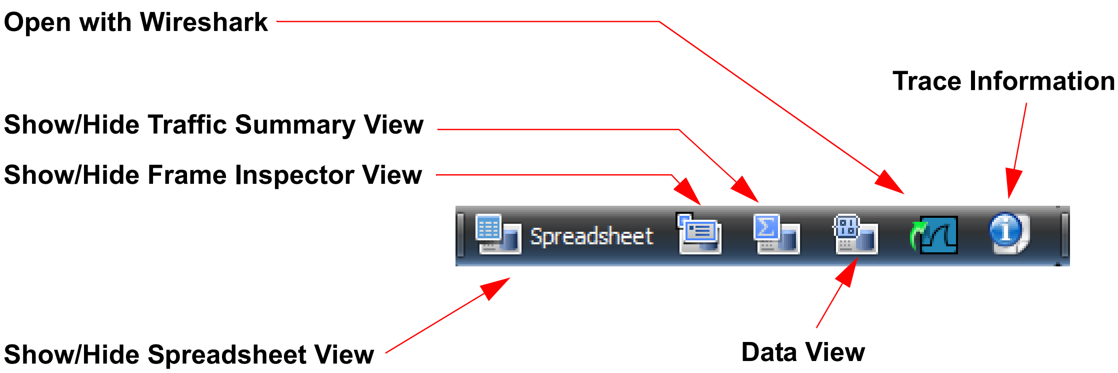

Open with Wireshark
Trace Information
Show/Hide Traffic Summary View
Show/Hide Frame Inspector View
Spreadsheet
Show/Hide Spreadsheet View
Data View

Figure 3.7: Analysis Toolbar.

After you select a view, it appears in a separate window. To increase the new window display size, use Zoom in and Zoom out from the View menu item or the buttons from the View Toolbar.

To rearrange the tiling, select the **Window** menu and choose **Window Cascade** or **Window Tile.**

3.3.1 Decoding Assignments

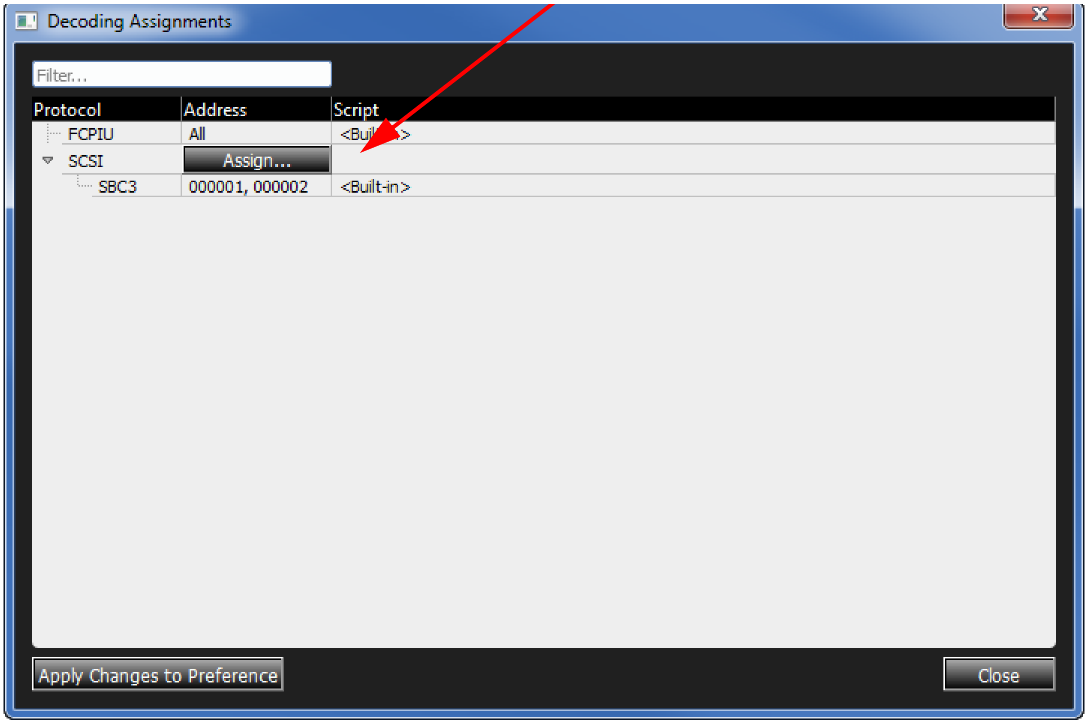
Click **Analysis> Decoding Assignments** to display the Decoding Assignments dialog. Click Assign to display the SCSI Assignment dialog (see Figure 3.9). Select an address and click **Close**.

The Script column identifies the script that will be used to decode the protocol.

<Built-in> means that a built-in decoder will be used.

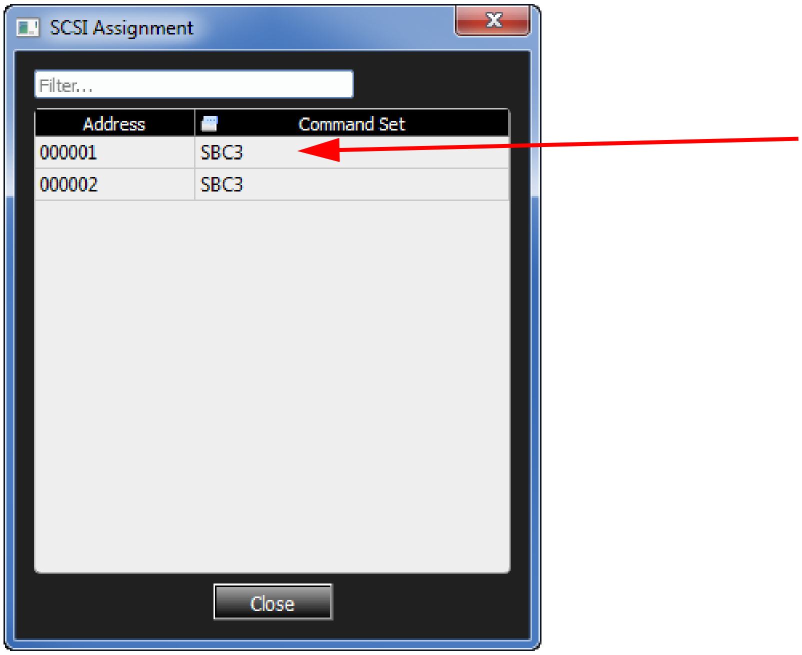
If you double-click in the cell, you can specify the path to a user-defined script (.udd).

See the Net Protocol Suite User-Defined Decoding manual for details on how to write a decoding script.



Protocol	Address	Script
FCPIU	All	<Built-in>
SCSI	Assign...	
SBC3	000001, 000002	<Built-in>

Figure 3.8: Decoding Assignments Dialog.



Address	Command Set
000001	SBC3
000002	SBC3

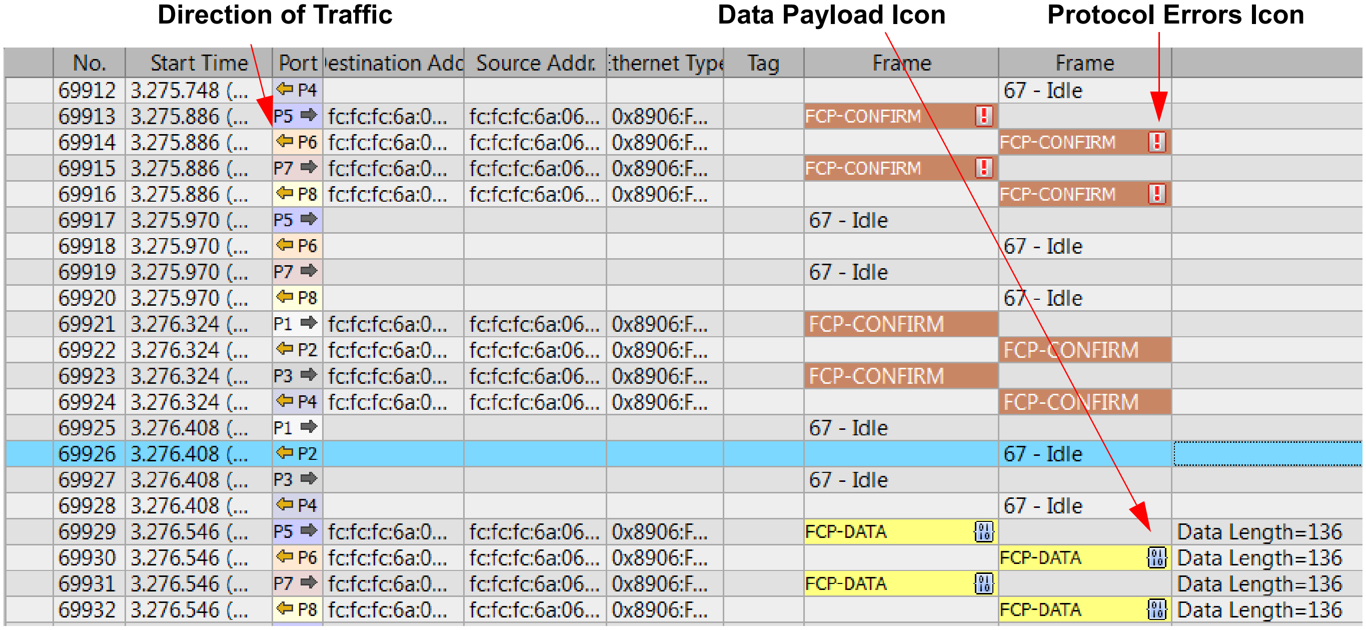
Figure 3.9: SCSI Assignment Dialog.

3.3.2 Spreadsheet View

The Spreadsheet View displays captured packets sequentially, one per line. The packets are decoded and packet fields are displayed column by column.

To display the Spreadsheet View of the current capture, click

Analysis > Spreadsheet View or click the Spreadsheet button on the View toolbar.


Direction of Traffic

Data Payload Icon

Protocol Errors Icon

	No.	Start Time	Port	estination Adc	Source Addr.	thernet Type	Tag	Frame	Frame	
	69912	3.275.748 (...	⇦ P4						67 - Idle	
	69913	3.275.886 (...	P5 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-CONFIRM ❗		
	69914	3.275.886 (...	⇦ P6	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-CONFIRM ❗	
	69915	3.275.886 (...	P7 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-CONFIRM ❗		
	69916	3.275.886 (...	⇦ P8	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-CONFIRM ❗	
	69917	3.275.970 (...	P5 ⇨					67 - Idle		
	69918	3.275.970 (...	⇦ P6						67 - Idle	
	69919	3.275.970 (...	P7 ⇨					67 - Idle		
	69920	3.275.970 (...	⇦ P8						67 - Idle	
	69921	3.276.324 (...	P1 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-CONFIRM		
	69922	3.276.324 (...	⇦ P2	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-CONFIRM	
	69923	3.276.324 (...	P3 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-CONFIRM		
	69924	3.276.324 (...	⇦ P4	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-CONFIRM	
	69925	3.276.408 (...	P1 ⇨					67 - Idle		
	69926	3.276.408 (...	⇦ P2						67 - Idle	
	69927	3.276.408 (...	P3 ⇨					67 - Idle		
	69928	3.276.408 (...	⇦ P4						67 - Idle	
	69929	3.276.546 (...	P5 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-DATA ▦		Data Length=136
	69930	3.276.546 (...	⇦ P6	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-DATA ▦	Data Length=136
	69931	3.276.546 (...	P7 ⇨	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...		FCP-DATA ▦		Data Length=136
	69932	3.276.546 (...	⇦ P8	fc:fc:fc:6a:0...	fc:fc:fc:6a:06...	0x8906:F...			FCP-DATA ▦	Data Length=136

Figure 3.10: Spreadsheet View.

Data Payload

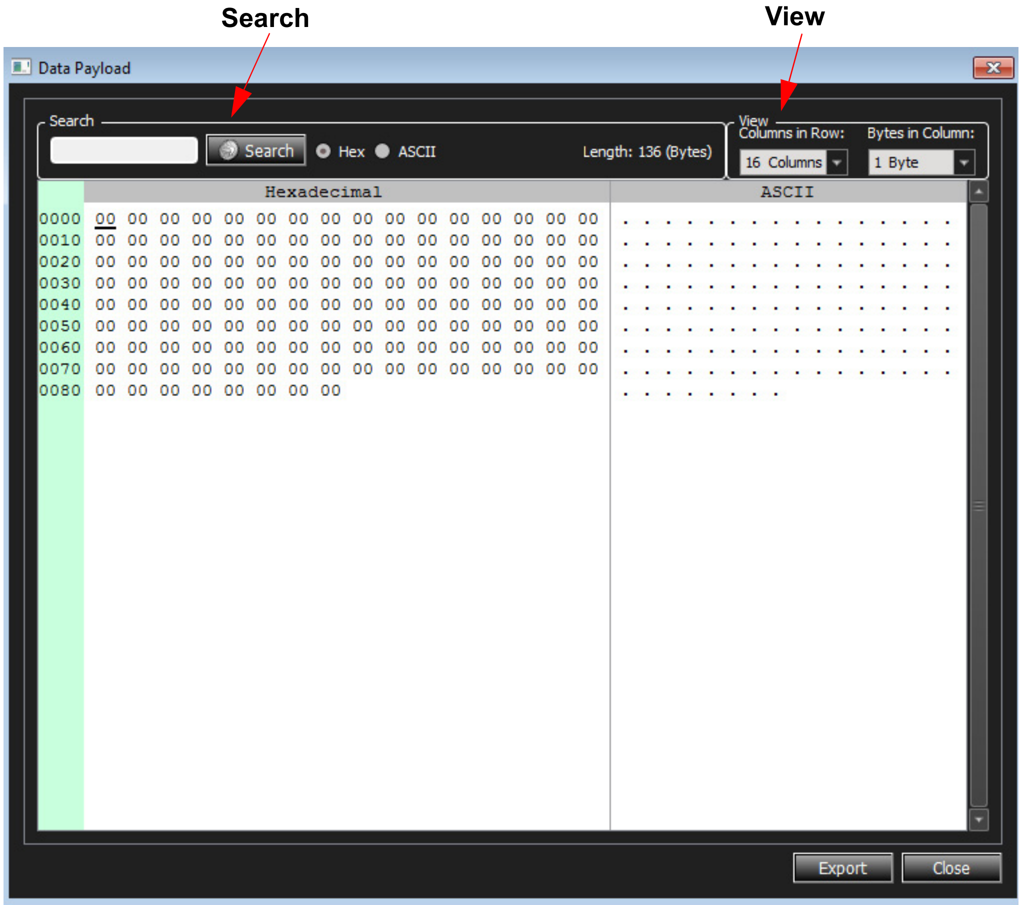
Click the ▦ icon to display the Data Payload dialog (see Figure 3.11 on page 120).

Click the **Export** button to export the data payload to a text file.

Enter a value and click the **Next** or **Previous** button to search the data payload in Hexadecimal or ASCII format. The application looks for byte boundaries while searching. Hence, searching for ‘1A’ will not result in a match because it spans two bytes, whereas searching for ‘01AC’ will result in a match (see Figure 3.12 on page 120).

Click the **Columns in Row** and **Bytes in Column** drop-down menu lists in the View pane to configure the display.

Click **Hex** or **ASCII** to specify the search criteria.



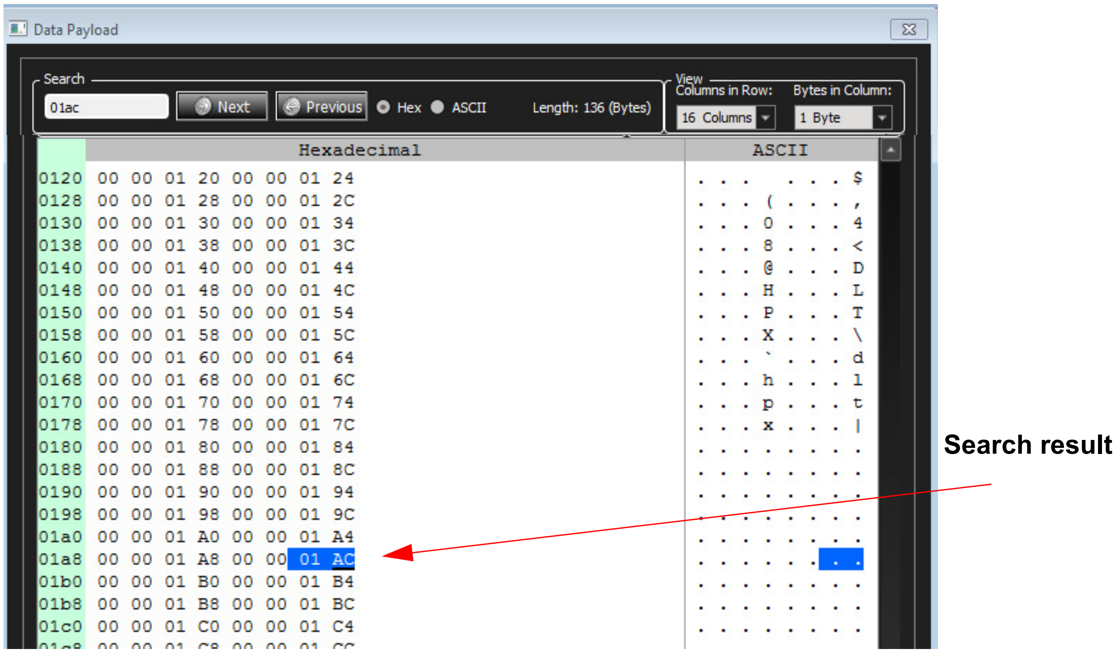
Search: [ ] Search ● Hex ● ASCII Length: 136 (Bytes)

View — Columns in Row: 16 Columns — Bytes in Column: 1 Byte

```
     Hexadecimal                                        ASCII
0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    . . . . . . . . . . . . . . . .
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    . . . . . . . . . . . . . . . .
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    . . . . . . . . . . . . . . . .
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    . . . . . . . . . . . . . . . .
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    . . . . . . . . . . . . . . . .
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    . . . . . . . . . . . . . . . .
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    . . . . . . . . . . . . . . . .
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    . . . . . . . . . . . . . . . .
0080 00 00 00 00 00 00 00 00                            . . . . . . . .
```

Figure 3.11: Data Payload Dialog.

Click the **Columns in Row** and **Bytes in Column** drop-down menu lists in the View pane to configure the display.



Search: 01ac ● Hex ● ASCII Length: 136 (Bytes)

View — Columns in Row: 16 Columns — Bytes in Column: 1 Byte

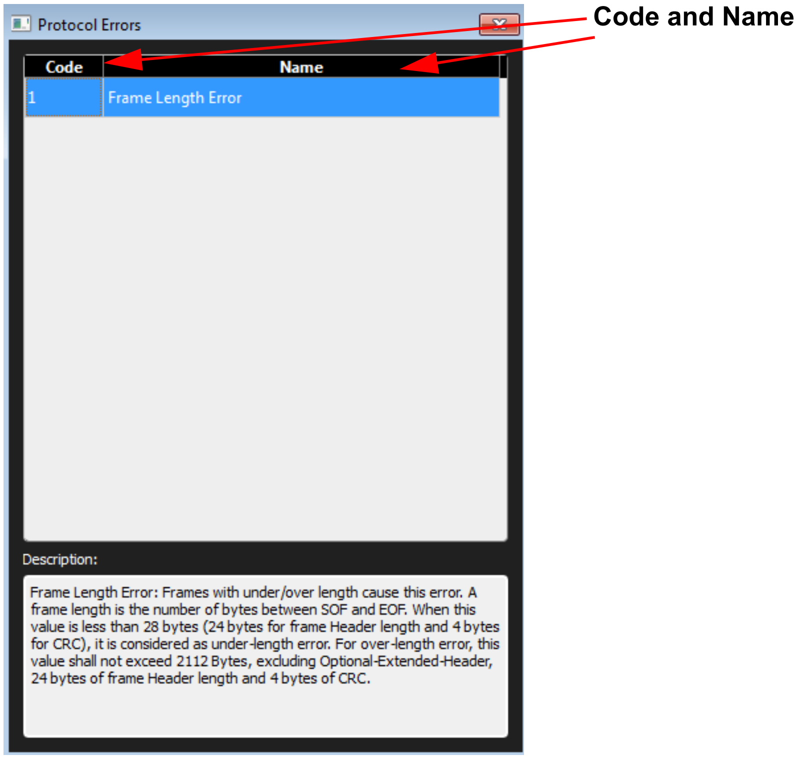
```
     Hexadecimal                  ASCII
0120 00 00 01 20 00 00 01 24      . . . .   . . . $
0128 00 00 01 28 00 00 01 2C      . . . ( . . . ,
0130 00 00 01 30 00 00 01 34      . . . 0 . . . 4
0138 00 00 01 38 00 00 01 3C      . . . 8 . . . <
0140 00 00 01 40 00 00 01 44      . . . @ . . . D
0148 00 00 01 48 00 00 01 4C      . . . H . . . L
0150 00 00 01 50 00 00 01 54      . . . P . . . T
0158 00 00 01 58 00 00 01 5C      . . . X . . . \
0160 00 00 01 60 00 00 01 64      . . . ` . . . d
0168 00 00 01 68 00 00 01 6C      . . . h . . . l
0170 00 00 01 70 00 00 01 74      . . . p . . . t
0178 00 00 01 78 00 00 01 7C      . . . x . . . |
0180 00 00 01 80 00 00 01 84      . . . . . . . .
0188 00 00 01 88 00 00 01 8C      . . . . . . . .
0190 00 00 01 90 00 00 01 94      . . . . . . . .
0198 00 00 01 98 00 00 01 9C      . . . . . . . .
01a0 00 00 01 A0 00 00 01 A4      . . . . . . . .
01a8 00 00 01 A8 00 00 01 AC      . . . . . . . .
01b0 00 00 01 B0 00 00 01 B4      . . . . . . . .
01b8 00 00 01 B8 00 00 01 BC      . . . . . . . .
01c0 00 00 01 C0 00 00 01 C4      . . . . . . . .
01c8 00 00 01 C8 00 00 01 CC
```

Figure 3.12: Data Payload Search Result.

Protocol Errors

Click the ❗ icon to display the Protocol Errors dialog (see Figure 3.13 on page 121).

It displays the Code and Name.



Code and Name

Code	Name
1	Frame Length Error

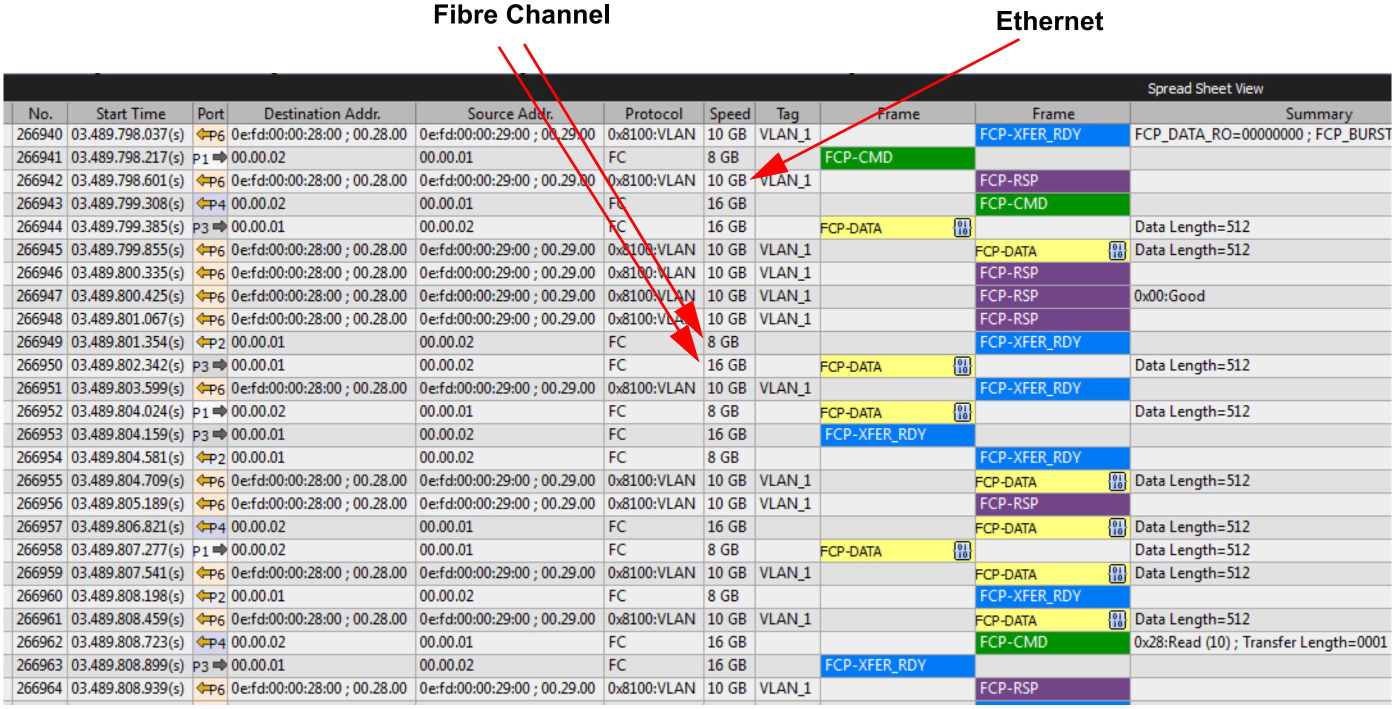
Description:

Frame Length Error: Frames with under/over length cause this error. A frame length is the number of bytes between SOF and EOF. When this value is less than 28 bytes (24 bytes for frame Header length and 4 bytes for CRC), it is considered as under-length error. For over-length error, this value shall not exceed 2112 Bytes, excluding Optional-Extended-Header, 24 bytes of frame Header length and 4 bytes of CRC.

Figure 3.13: Protocol Error Dialog.

Viewing Ethernet and Fibre Channel Traces

The application captures and displays both Ethernet and Fibre Channel data.



No.	Start Time	Port	Destination Addr.	Source Addr.	Protocol	Speed	Tag	Frame	Frame	Summary
266940	03.489.798.037(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-XFER_RDY	FCP_DATA_RO=00000000 ; FCP_BURST
266941	03.489.798.217(s)	P1⇨	00.00.02	00.00.01	FC	8 GB		FCP-CMD		
266942	03.489.798.601(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	
266943	03.489.799.308(s)	⇦P4	00.00.02	00.00.01	FC	16 GB			FCP-CMD	
266944	03.489.799.385(s)	P3⇨	00.00.01	00.00.02	FC	16 GB		FCP-DATA		Data Length=512
266945	03.489.799.855(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-DATA	Data Length=512
266946	03.489.800.335(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	
266947	03.489.800.425(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	0x00:Good
266948	03.489.801.067(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	
266949	03.489.801.354(s)	⇦P2	00.00.01	00.00.02	FC	8 GB			FCP-XFER_RDY	
266950	03.489.802.342(s)	P3⇨	00.00.01	00.00.02	FC	16 GB		FCP-DATA		Data Length=512
266951	03.489.803.599(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-XFER_RDY	
266952	03.489.804.024(s)	P1⇨	00.00.02	00.00.01	FC	8 GB		FCP-DATA		Data Length=512
266953	03.489.804.159(s)	P3⇨	00.00.01	00.00.02	FC	16 GB		FCP-XFER_RDY		
266954	03.489.804.581(s)	⇦P2	00.00.01	00.00.02	FC	8 GB			FCP-XFER_RDY	
266955	03.489.804.709(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-DATA	Data Length=512
266956	03.489.805.189(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	
266957	03.489.806.821(s)	⇦P4	00.00.02	00.00.01	FC	16 GB			FCP-DATA	Data Length=512
266958	03.489.807.277(s)	P1⇨	00.00.02	00.00.01	FC	8 GB		FCP-DATA		Data Length=512
266959	03.489.807.541(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-DATA	Data Length=512
266960	03.489.808.198(s)	⇦P2	00.00.01	00.00.02	FC	8 GB			FCP-XFER_RDY	
266961	03.489.808.459(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-DATA	Data Length=512
266962	03.489.808.723(s)	⇦P4	00.00.02	00.00.01	FC	16 GB			FCP-CMD	0x28:Read (10) ; Transfer Length=0001
266963	03.489.808.899(s)	P3⇨	00.00.01	00.00.02	FC	16 GB		FCP-XFER_RDY		
266964	03.489.808.939(s)	⇦P6	0e:fd:00:00:28:00 ; 00.28.00	0e:fd:00:00:29:00 ; 00.29.00	0x8100:VLAN	10 GB	VLAN_1		FCP-RSP	

Figure 3.14: Merged FC and Ethernet Traces in Spreadsheet View.

Save As and Export

Select **File > Save As** to open the Save As dialog. Refer to “Saving a Trace Capture” on page 68 and “Exporting a Trace Capture” on page 69.

Spreadsheet View Menu Options

Right-click on any of the columns in the Spreadsheet view to display a list of menu options (see Figure).

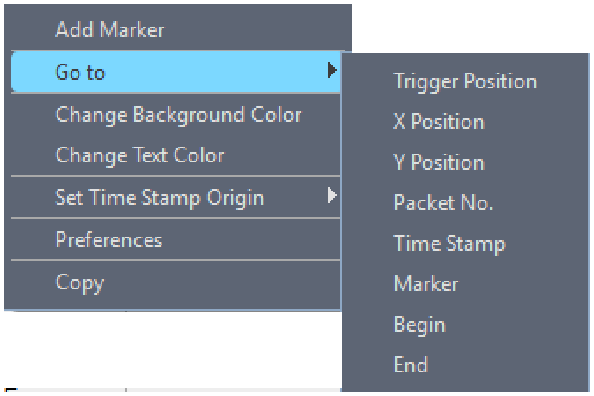


Figure 3.15: Right-click Menu Options in Spreadsheet View.

Add Marker	Opens the Marker List dialog. You can add and delete markers (see “Markers” on page 127.)
Byte Order	This option is context sensitive. This option allows a you left/right align the data display in each cell.
Go to:	The Go to option jumps to a related frame in the viewer. It displays the following sub-menu options to go to Trigger, X or Y Position, Packet No., Time Stamp, Marker, Begin and End.
Change Background Color:	Displays colors to change the background.
Change Text Color:	Displays colors to change the text.
Set Time Stamp Origin:	There are four options to set time stamp origin.
•Absolute:	Sets the time stamp to zero when the recording starts. The first frame in the trace might have the time stamp larger than zero due to filtering, hiding or other reasons such as recording started in the middle of a frame.
•Trigger:	Sets time to when the trace was triggered.
•Current Position:	Sets time to the current position.
•Based on System Time:	Sets time based on the system time.
Preferences	Displays the Preferences dialog.
Copy	Copies the frame to allow you to paste it in the Trigger settings.

Column Display Options

You can customize the columns display by showing/hiding, adding, editing or deleting columns. Right-click on the column header and select an option as shown in Figure 3.16 on page 123.

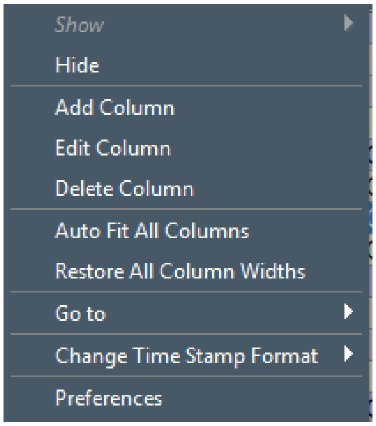
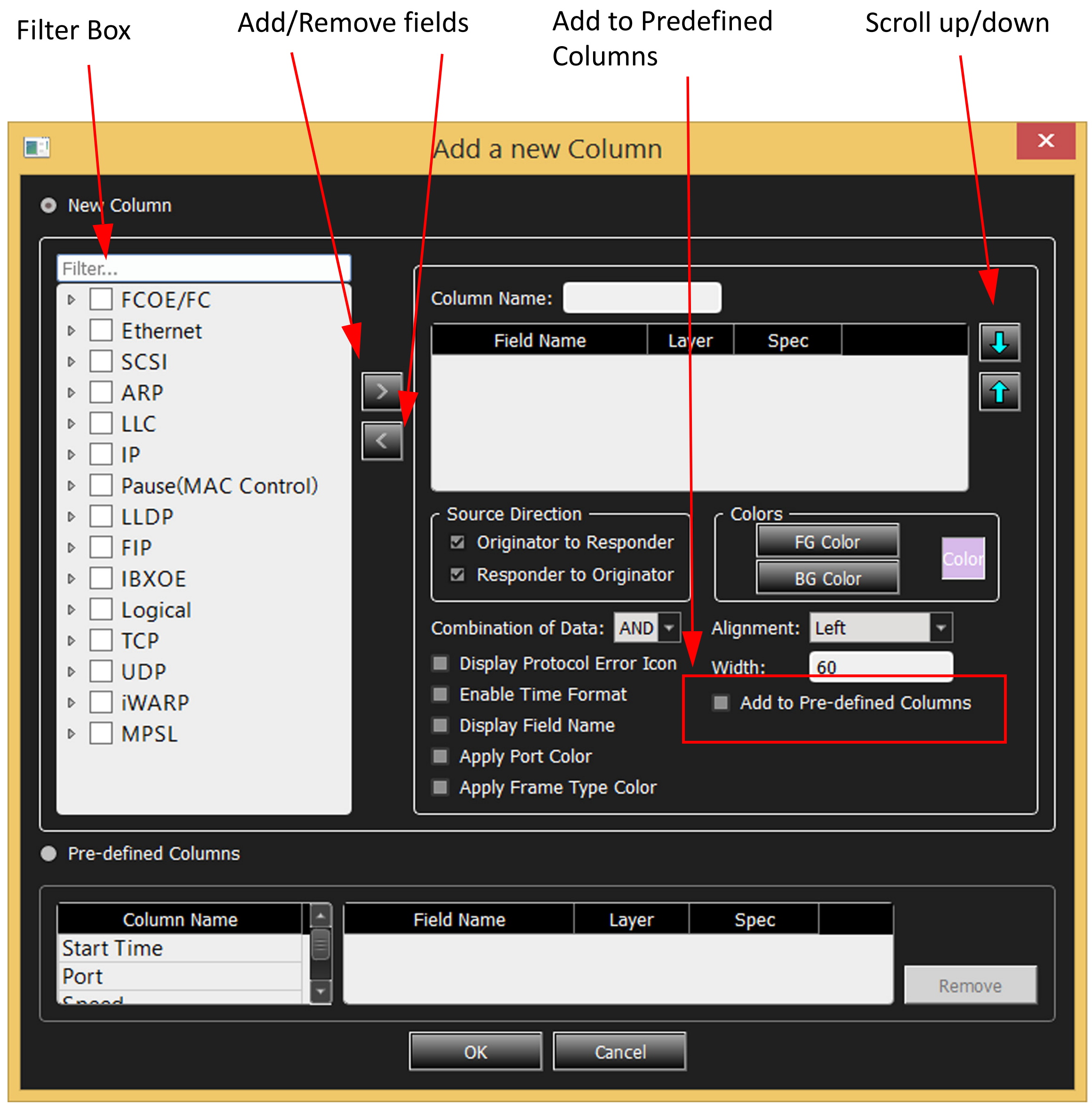


Figure 3.16: Right-click Menu Options in Spreadsheet View.

Show	Displays a hidden column.
Hide	Hides a column.
Add Column	Allows you to add a column (see Figure 3.17 on page 125). Select Field, Column Name, Source Direction, foreground and back ground Colors, choose And/OR, display Data Payload Protocol Error icons, apply Frame and Port color, enable Time Format, display Field name, set column Alignment and Width and Add to Pre-defined Columns. Columns can also be added to the Pre-defined columns list. This list is a flat list where you can keep columns you might want to toggle on/off.
Edit Column	Allows you to edit column properties. It has the same functionality as Add Column above (see Figure 3.18 on page 126).
Delete Column	Allows you to delete the selected column.
Auto Fit All Columns	Adjusts the column widths to fit the text.
Restore All Columns Widths	Restores the column widths to the previous size.
Go to:	Displays options to go to Trigger, X or Y Position, Packet No., Time Stamp, Marker, Begin and End.
Change Time Stamp Format:	Displays options to select the time stamp format.
Preferences	Displays the Preferences dialog.

Selecting **Add Column** displays the following dialog.



☑ Originator to Responder

☑ Responder to Originator

Combination of Data: AND

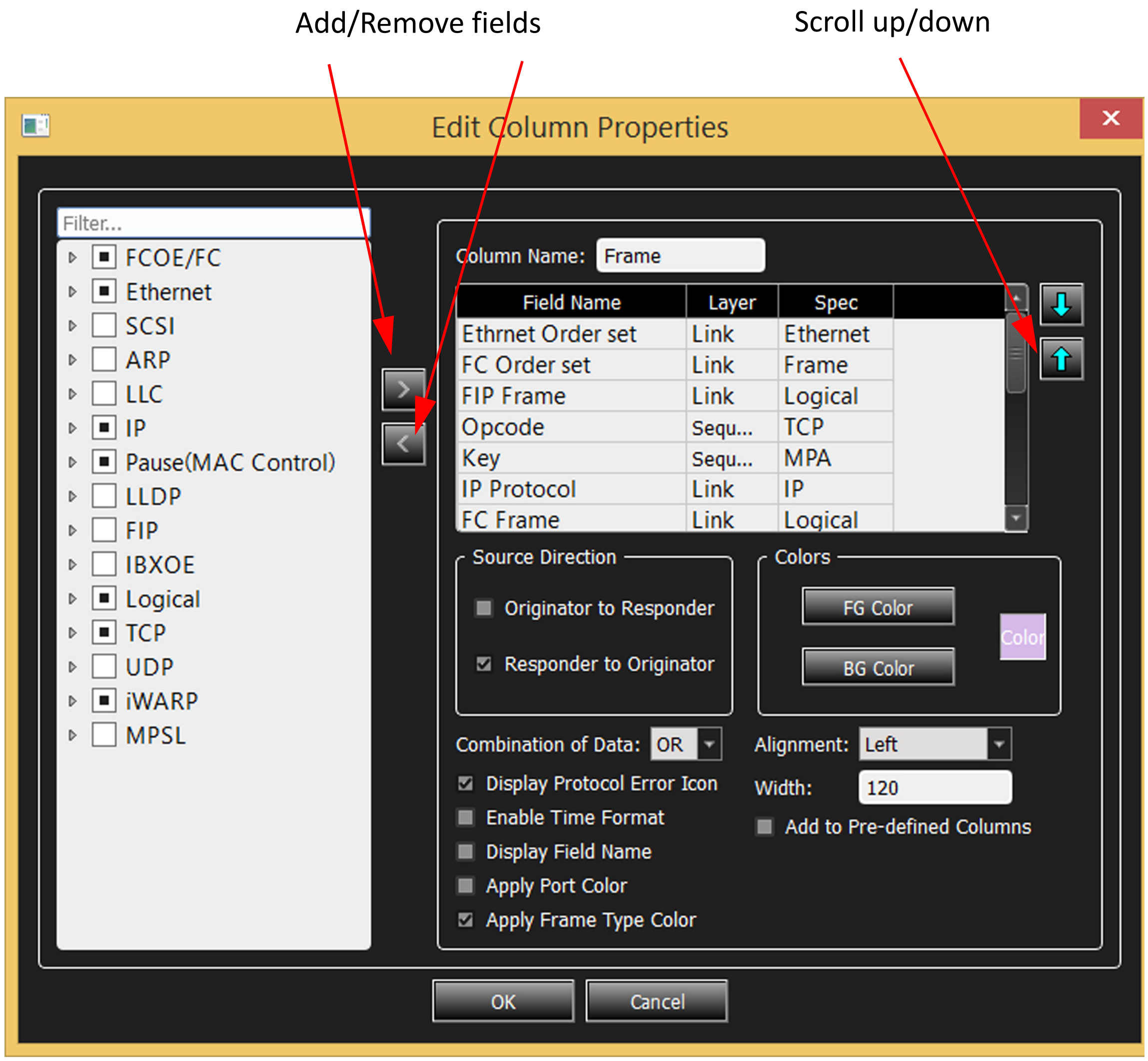
Alignment: Left

Width: 60

Figure 3.17: Add a New Column Dialog.

You can select any combination of fields to fill the content of the column. Use the Filter text box above the Fields tree list to more easily find the fields you're interested in. In case you select multiple fields, the up/down buttons enable you to specify in which order they should be displayed in the column. Desired columns can also be added to the pre-defined columns. Pre-defined columns are ones that contain metadata (such as timestamp, port number, etc.) or custom ones that have been added by checking the "Add to Predefined Column" checkbox.

Selecting **Edit Column** displays the following dialog.



- ■ FCOE/FC
- ■ Ethernet
- □ SCSI
- □ ARP
- □ LLC
- ■ IP
- ■ Pause(MAC Control)
- □ LLDP
- □ FIP
- □ IBXOE
- ■ Logical
- ■ TCP
- □ UDP
- ■ iWARP
- □ MPSL

Column Name: Frame

Field Name	Layer	Spec
Ethrnet Order set	Link	Ethernet
FC Order set	Link	Frame
FIP Frame	Link	Logical
Opcode	Sequ...	TCP
Key	Sequ...	MPA
IP Protocol	Link	IP
FC Frame	Link	Logical

Source Direction

□ Originator to Responder

☑ Responder to Originator

Colors

Combination of Data: OR

Alignment: Left

Width: 120

☑ Display Protocol Error Icon

□ Enable Time Format

□ Display Field Name

□ Apply Port Color

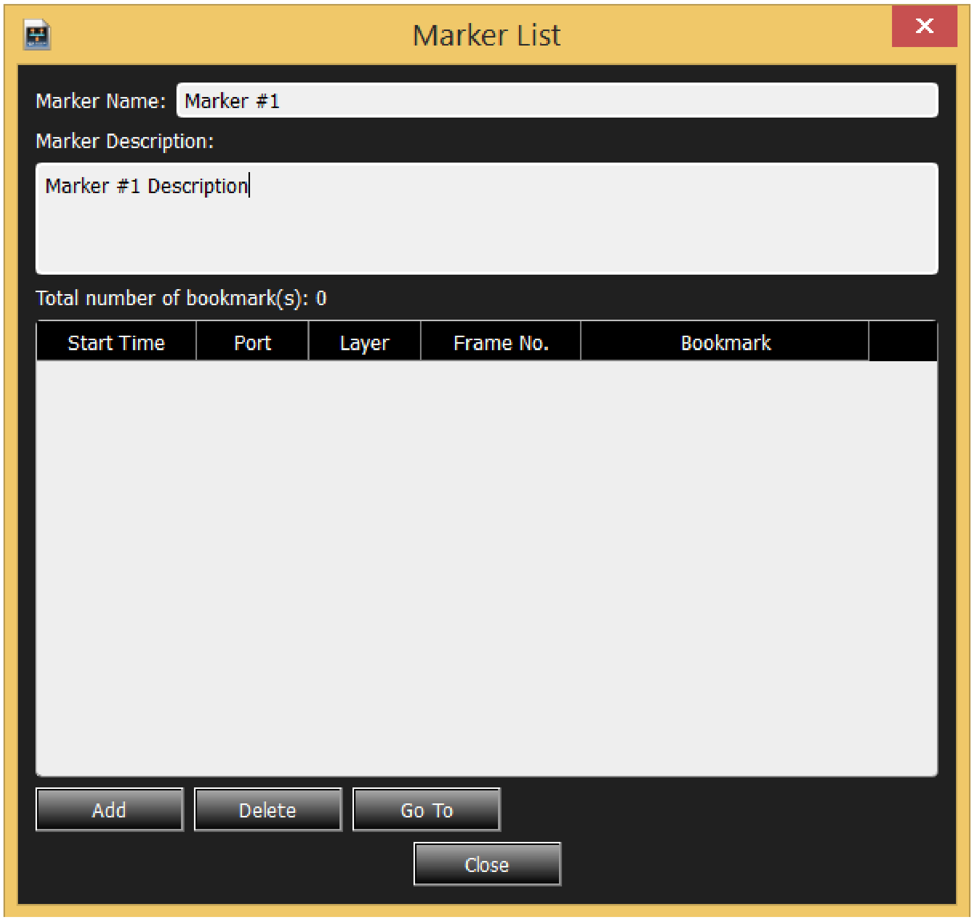
☑ Apply Frame Type Color

□ Add to Pre-defined Columns

Figure 3.18: Edit Column Properties Dialog.

Markers

Markers are a convenient way to mark a point in the spreadsheet by name, so that you can rapidly return to that point. You can create markers for your data by right-clicking any where in the data in Spreadsheet view (see figure below) and select **Add Marker** (see Figure 3.19 on page 127). Enter a Name and description click **Add**. You can also delete, edit or go to a specific marker.



Marker List

Marker Name: Marker #1

Marker Description:

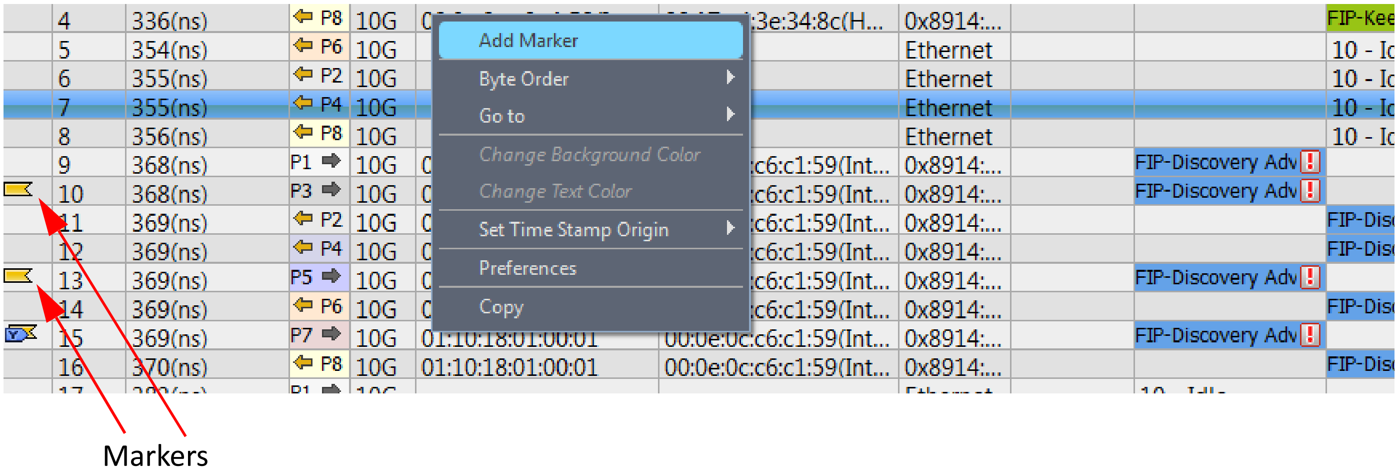
Marker #1 Description

Total number of bookmark(s): 0

Start Time	Port	Layer	Frame No.	Bookmark

Figure 3.19: Marker List Dialog

Once markers are created they display in the left column of the rows as shown below. Right-click on the marked row and select **Edit Marker** to edit it. Click the **Delete** button to delete the marker.



	4	336(ns)	⇦ P8	10G	0	:3e:34:8c(H...	0x8914:...			FIP-Kee
	5	354(ns)	⇦ P6	10G			Ethernet			10 - Ic
	6	355(ns)	⇦ P2	10G			Ethernet			10 - Ic
	7	355(ns)	⇦ P4	10G			Ethernet			10 - Ic
	8	356(ns)	⇦ P8	10G			Ethernet			10 - Ic
	9	368(ns)	P1 ⇨	10G	0	:c6:c1:59(Int...	0x8914:...		FIP-Discovery Adv !	
⚑	10	368(ns)	P3 ⇨	10G	0	:c6:c1:59(Int...	0x8914:...		FIP-Discovery Adv !	
	11	369(ns)	⇦ P2	10G	0	:c6:c1:59(Int...	0x8914:...			FIP-Dis
	12	369(ns)	⇦ P4	10G	0	:c6:c1:59(Int...	0x8914:...			FIP-Dis
⚑	13	369(ns)	P5 ⇨	10G	0	:c6:c1:59(Int...	0x8914:...		FIP-Discovery Adv !	
	14	369(ns)	⇦ P6	10G	0	:c6:c1:59(Int...	0x8914:...			FIP-Dis
⚑	15	369(ns)	P7 ⇨	10G	01:10:18:01:00:01	00:0e:0c:c6:c1:59(Int...	0x8914:...		FIP-Discovery Adv !	
	16	370(ns)	⇦ P8	10G	01:10:18:01:00:01	00:0e:0c:c6:c1:59(Int...	0x8914:...			FIP-Dis

Figure 3.20: Markers in Spreadsheet View

Finding a Marker

To find a marker in the right-click the mouse in the trace viewer and select **Go to > Marker**.

Highlight the bookmark to which to go, then click the **Go To** button, or double-click the selection**.**

Marker Description

To get a quick description of a displayed bookmark, position the tool tip over a bookmark. The name and description of the bookmark display.

3.3.3 Frame Inspector View

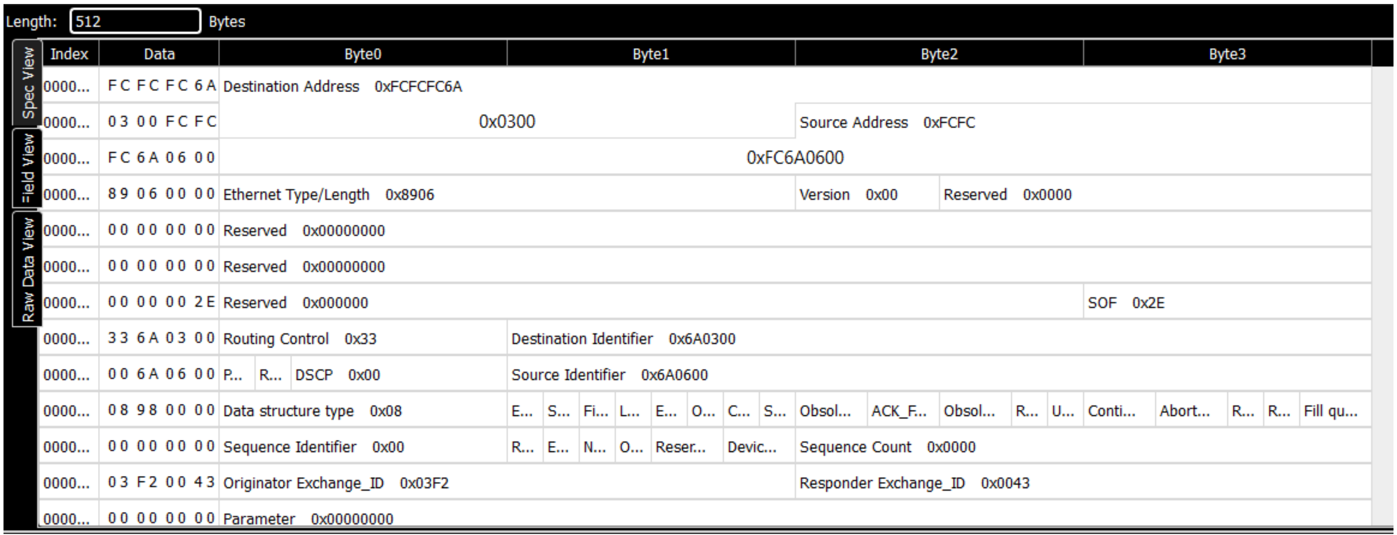
Frame Inspector View has lots of information that is available in Packet View, but not Spreadsheet View, so it is most useful in conjunction with the Spreadsheet View.

To open a Frame Inspector View of the current capture, select **Analysis > Frame Inspector View** or click the 🗔 button on the View Type toolbar.

This Frame Inspector View has the following three tabs:

Spec View

This view shows the Frame as it would appear in the spec, with the field names and values spelled out clearly. Fields that are too short to clearly contain the description can be viewed as tooltips by hovering the mouse over them. Some fields might have a a lowercase ‘e’ button at the top right corner. Pressing this button displays an ‘expanded’ view of the sub-fields in this field.



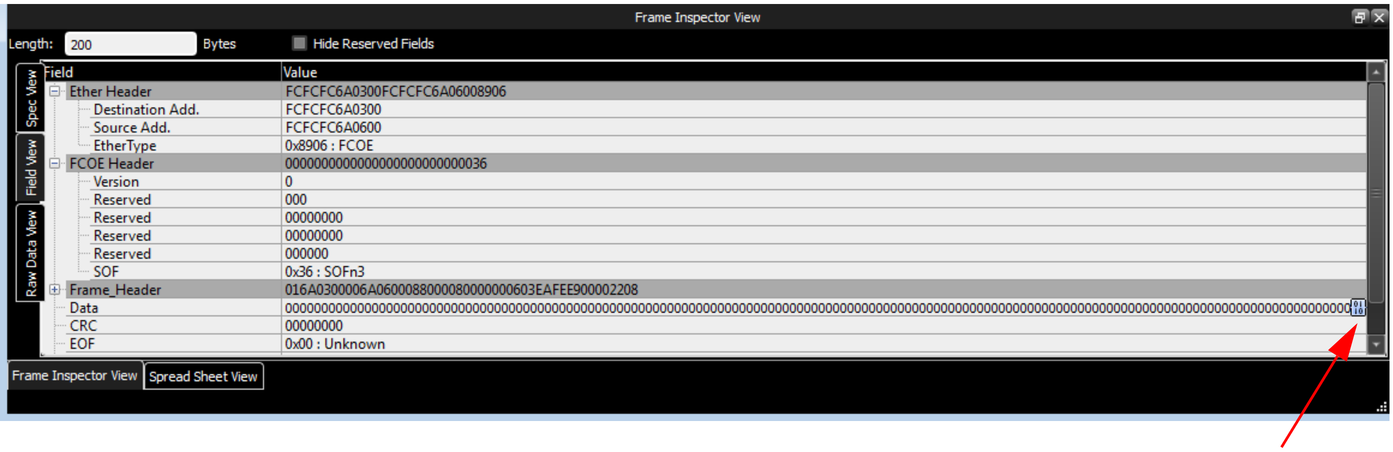
Length: 512 Bytes

Index	Data	Byte0	Byte1	Byte2	Byte3
0000...	FC FC FC 6A	Destination Address 0xFCFCFC6A			
0000...	03 00 FC FC	0x0300		Source Address 0xFCFC	
0000...	FC 6A 06 00	0xFC6A0600			
0000...	89 06 00 00	Ethernet Type/Length 0x8906		Version 0x00 Reserved 0x0000	
0000...	00 00 00 00	Reserved 0x00000000			
0000...	00 00 00 00	Reserved 0x00000000			
0000...	00 00 00 2E	Reserved 0x000000			SOF 0x2E
0000...	33 6A 03 00	Routing Control 0x33	Destination Identifier 0x6A0300		
0000...	00 6A 06 00	P... R... DSCP 0x00	Source Identifier 0x6A0600		
0000...	08 98 00 00	Data structure type 0x08	E... S... Fi... L... E... O... C... S...	Obsol... ACK_F... Obsol... R... U...	Conti... Abort... R... R... Fill qu...
0000...	00 00 00 00	Sequence Identifier 0x00	R... E... N... O... Reser... Devic...	Sequence Count 0x0000	
0000...	03 F2 00 43	Originator Exchange_ID 0x03F2		Responder Exchange_ID 0x0043	
0000...	00 00 00 00	Parameter 0x00000000			

Figure 3.21: Frame Inspector-Spec View

Field View

This view shows, when applicable, a hierarchical display of the selected Packet, with the relevant fields in each level.



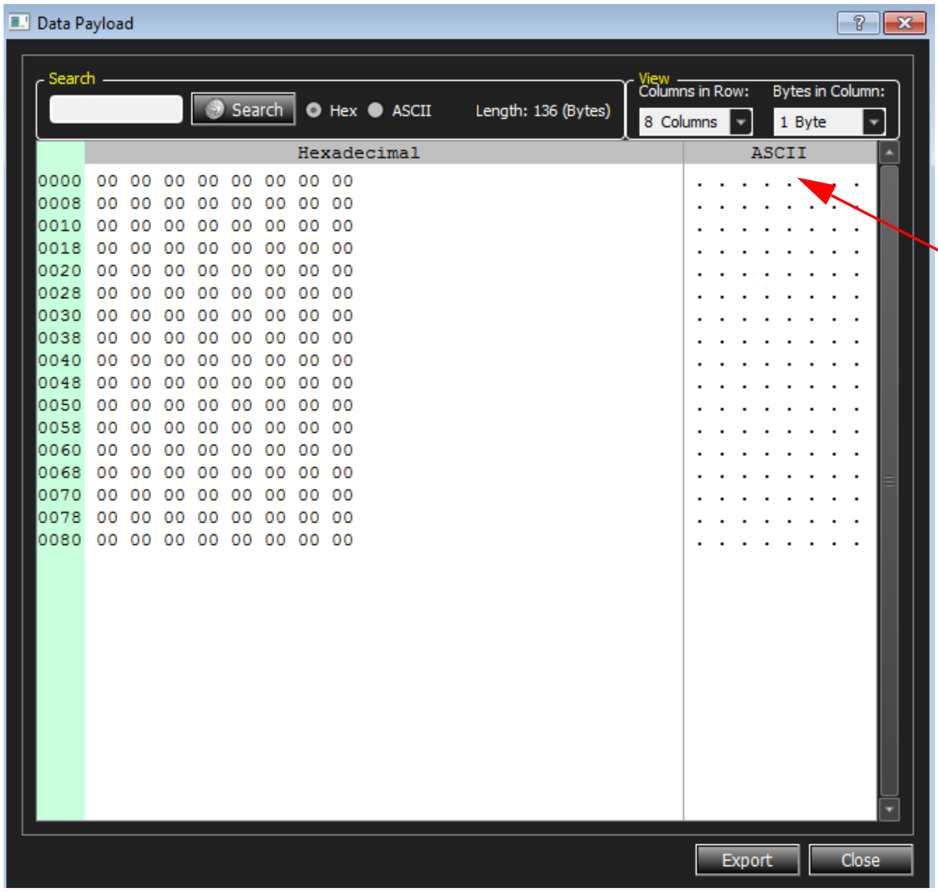
Length: 200 Bytes ■ Hide Reserved Fields

Field	Value
⊟ Ether Header	FCFCFC6A0300FCFCFC6A06008906
Destination Add.	FCFCFC6A0300
Source Add.	FCFCFC6A0600
EtherType	0x8906 : FCOE
⊟ FCOE Header	000000000000000000000000036
Version	0
Reserved	000
Reserved	00000000
Reserved	00000000
Reserved	000000
SOF	0x36 : SOFn3
⊞ Frame_Header	016A0300006A0600088000080000000603EAFEE900002208
Data	00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
CRC	00000000
EOF	0x00 : Unknown

Data Payload Button

Figure 3.22: Frame Inspector-Field View

Click the Data Payload button to display the Data Payload dialog (see Figure 3.23 on page 130).



○ Hex ● ASCII

Length: 136 (Bytes)

View

Columns in Row: 8 Columns

Bytes in Column: 1 Byte

```
     Hexadecimal                ASCII
0000 00 00 00 00 00 00 00 00    . . . . . . . .
0008 00 00 00 00 00 00 00 00    . . . . . . . .
0010 00 00 00 00 00 00 00 00    . . . . . . . .
0018 00 00 00 00 00 00 00 00    . . . . . . . .
0020 00 00 00 00 00 00 00 00    . . . . . . . .
0028 00 00 00 00 00 00 00 00    . . . . . . . .
0030 00 00 00 00 00 00 00 00    . . . . . . . .
0038 00 00 00 00 00 00 00 00    . . . . . . . .
0040 00 00 00 00 00 00 00 00    . . . . . . . .
0048 00 00 00 00 00 00 00 00    . . . . . . . .
0050 00 00 00 00 00 00 00 00    . . . . . . . .
0058 00 00 00 00 00 00 00 00    . . . . . . . .
0060 00 00 00 00 00 00 00 00    . . . . . . . .
0068 00 00 00 00 00 00 00 00    . . . . . . . .
0070 00 00 00 00 00 00 00 00    . . . . . . . .
0078 00 00 00 00 00 00 00 00    . . . . . . . .
0080 00 00 00 00 00 00 00 00    . . . . . . . .
```

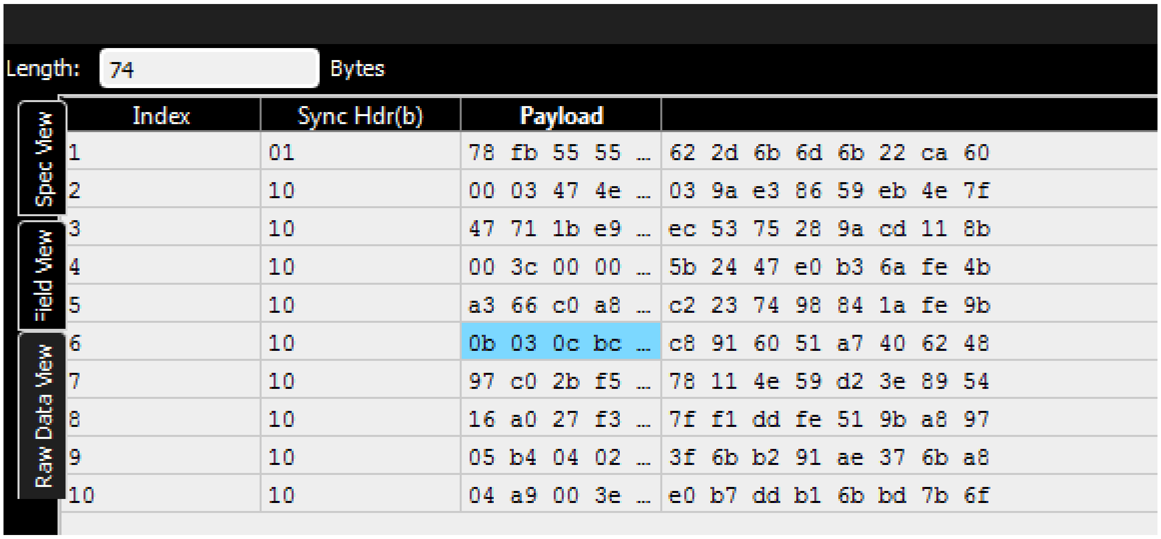
Figure 3.23: Data Payload Dialog

Any ASCII non-printable characters are depicted as black dots as shown above.

Raw Data View - Frame Inspector View for 64b/66b Decoding

Raw Data View in the **Frame Inspector View** window shows the exact bit stream in 66b format (see Figure on page 131). This view shows Hex, 10-bit and Running Disparity views of each dword in the selected packet. In this view, a 66 bits block is reconstructed similar to the received data (see the screen capture below). The following columns are displayed in the **Raw Data View**:

- **Index**: This column demonstrates the index of the 66-bits symbol in current blocks.
- **Sync Header**: This column shows the Sync Header bits of a symbol.
- **Payload**: This column shows the 8 payload bytes in each symbol before scrambling.
- **Scrambled**: This column shows the 8 payload bytes in each symbol after scrambling.



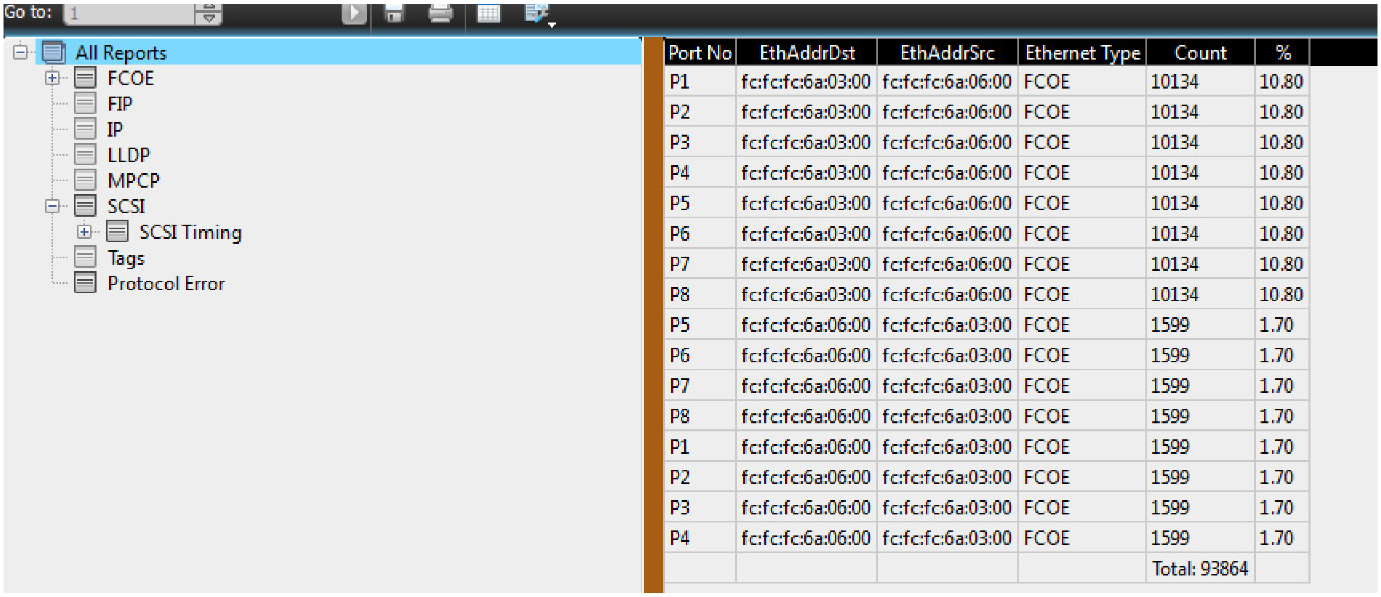
Length: 74 Bytes

Index	Sync Hdr(b)	Payload	
1	01	78 fb 55 55 ...	62 2d 6b 6d 6b 22 ca 60
2	10	00 03 47 4e ...	03 9a e3 86 59 eb 4e 7f
3	10	47 71 1b e9 ...	ec 53 75 28 9a cd 11 8b
4	10	00 3c 00 00 ...	5b 24 47 e0 b3 6a fe 4b
5	10	a3 66 c0 a8 ...	c2 23 74 98 84 1a fe 9b
6	10	0b 03 0c bc ...	c8 91 60 51 a7 40 62 48
7	10	97 c0 2b f5 ...	78 11 4e 59 d2 3e 89 54
8	10	16 a0 27 f3 ...	7f f1 dd fe 51 9b a8 97
9	10	05 b4 04 02 ...	3f 6b b2 91 ae 37 6b a8
10	10	04 a9 00 3e ...	e0 b7 dd b1 6b bd 7b 6f

Figure 3.24: Raw Data View without FEC

3.3.4 Traffic Summary View

The Analysis menu option allows you to run a traffic summary of the captured trace. The Traffic Summary View for each captured pattern can be viewed. This Summary View displays the port number, statistics and the percentage of the total count.

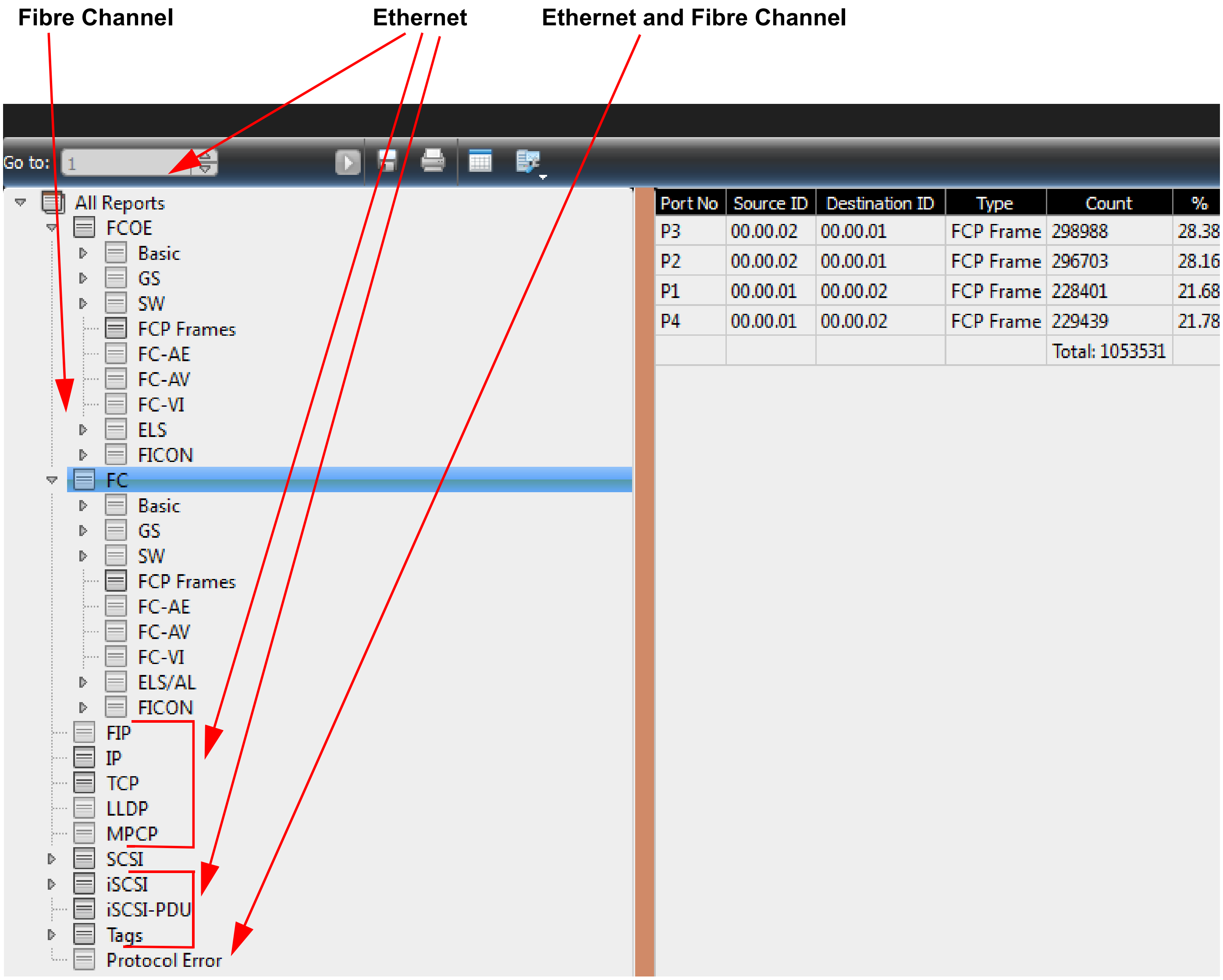


Port No	EthAddrDst	EthAddrSrc	Ethernet Type	Count	%
P1	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FCOE	10134	10.80
P2	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FCOE	10134	10.80
P3	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FCOE	10134	10.80
P4	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FCOE	10134	10.80
P5	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FCOE	10134	10.80
P6	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FCOE	10134	10.80
P7	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FCOE	10134	10.80
P8	fc:fc:fc:6a:03:00	fc:fc:fc:6a:06:00	FCOE	10134	10.80
P5	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FCOE	1599	1.70
P6	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FCOE	1599	1.70
P7	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FCOE	1599	1.70
P8	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FCOE	1599	1.70
P1	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FCOE	1599	1.70
P2	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FCOE	1599	1.70
P3	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FCOE	1599	1.70
P4	fc:fc:fc:6a:06:00	fc:fc:fc:6a:03:00	FCOE	1599	1.70
				Total: 93864	

Figure 3.25: Traffic Summary View

Viewing Ethernet and Fibre Channel Traces in Traffic Summary View

The application captures and displays both Ethernet and Fibre Channel data.



Fibre Channel

Ethernet

Ethernet and Fibre Channel

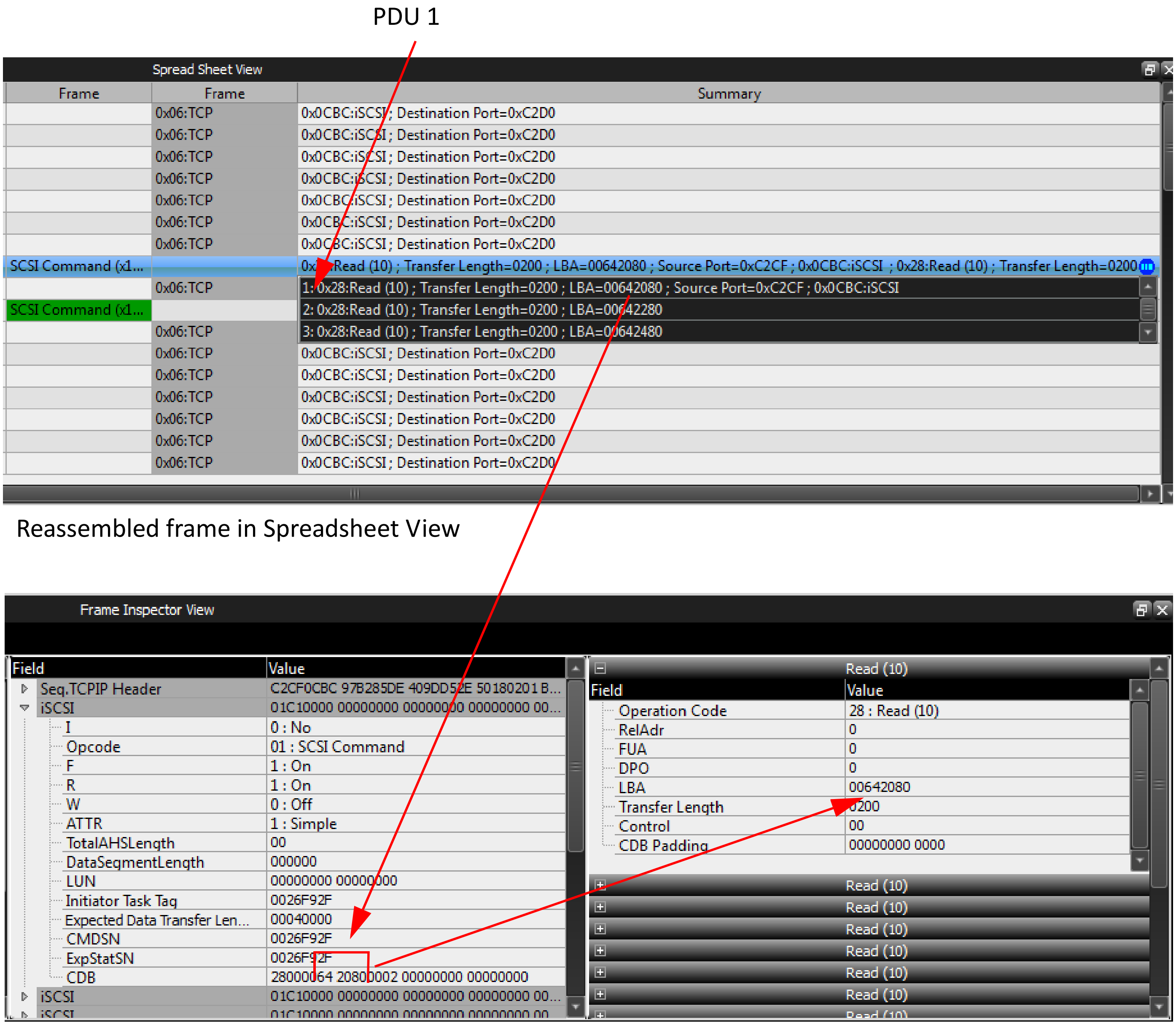
Port No	Source ID	Destination ID	Type	Count	%
P3	00.00.02	00.00.01	FCP Frame	298988	28.38
P2	00.00.02	00.00.01	FCP Frame	296703	28.16
P1	00.00.01	00.00.02	FCP Frame	228401	21.68
P4	00.00.01	00.00.02	FCP Frame	229439	21.78
				Total: 1053531	

Figure 3.26: Merged FC and Ethernet Traces in Traffic Summary View

3.3.5 Reassembly of Frames

Frames transmitted over the Ethernet break up into PDUs (Protocol Data Units). These PDUs may be received in a different order than they were originally transmitted. The application reassembles and displays them in the original order.

The screen captures below show the details of the reassembled frame in both the Spreadsheet View and the Frame Inspector View. The details of PDU1 in the Spreadsheet View are shown in the Frame Inspector View



Frame	Frame	Summary
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
SCSI Command (x1...		0x28:Read (10) ; Transfer Length=0200 ; LBA=00642080 ; Source Port=0xC2CF ; 0x0CBC:iSCSI ; 0x28:Read (10) ; Transfer Length=0200
	0x06:TCP	1: 0x28:Read (10) ; Transfer Length=0200 ; LBA=00642080 ; Source Port=0xC2CF ; 0x0CBC:iSCSI
SCSI Command (x1...		2: 0x28:Read (10) ; Transfer Length=0200 ; LBA=00642280
	0x06:TCP	3: 0x28:Read (10) ; Transfer Length=0200 ; LBA=00642480
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0
	0x06:TCP	0x0CBC:iSCSI ; Destination Port=0xC2D0

Reassembled frame in Spreadsheet View

Field	Value
Seq.TCPIP Header	C2CF0CBC 97B285DE 409DD52E 50180201 B...
iSCSI	01C10000 00000000 00000000 00000000 00...
I	0 : No
Opcode	01 : SCSI Command
F	1 : On
R	1 : On
W	0 : Off
ATTR	1 : Simple
TotalAHSLength	00
DataSegmentLength	000000
LUN	00000000 00000000
Initiator Task Tag	0026F92F
Expected Data Transfer Len...	00040000
CMDSN	0026F92F
ExpStatSN	0026F92F
CDB	28000064 20800002 00000000 00000000
iSCSI	01C10000 00000000 00000000 00000000 00...
iSCSI	01C10000 00000000 00000000 00000000 00...

Read (10)

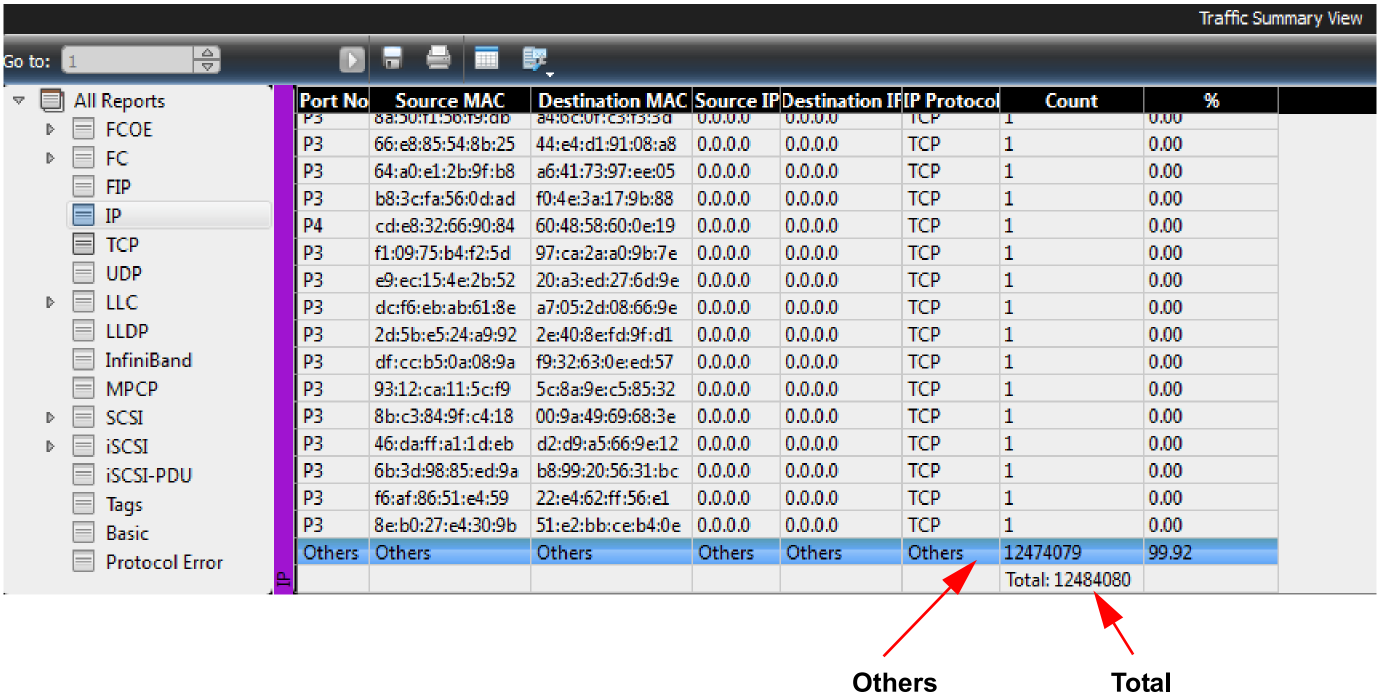
Field	Value
Operation Code	28 : Read (10)
RelAdr	0
FUA	0
DPO	0
LBA	00642080
Transfer Length	0200
Control	00
CDB Padding	00000000 0000

Reassembled frame in Frame Inspector View

Figure 3.27: Reassembled Frame.

3.3.6 Source and Destination Columns in Traffic Summary View

Traffic Summary displays the Source and Destination addresses for the first 10,000 pairs; the rest are grouped in the **Others** row.



Port No	Source MAC	Destination MAC	Source IP	Destination IP	IP Protocol	Count	%
P3	8a:50:f1:50:f9:db	a4:6c:0f:c3:f3:3d	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	66:e8:85:54:8b:25	44:e4:d1:91:08:a8	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	64:a0:e1:2b:9f:b8	a6:41:73:97:ee:05	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	b8:3c:fa:56:0d:ad	f0:4e:3a:17:9b:88	0.0.0.0	0.0.0.0	TCP	1	0.00
P4	cd:e8:32:66:90:84	60:48:58:60:0e:19	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	f1:09:75:b4:f2:5d	97:ca:2a:a0:9b:7e	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	e9:ec:15:4e:2b:52	20:a3:ed:27:6d:9e	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	dc:f6:eb:ab:61:8e	a7:05:2d:08:66:9e	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	2d:5b:e5:24:a9:92	2e:40:8e:fd:9f:d1	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	df:cc:b5:0a:08:9a	f9:32:63:0e:ed:57	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	93:12:ca:11:5c:f9	5c:8a:9e:c5:85:32	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	8b:c3:84:9f:c4:18	00:9a:49:69:68:3e	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	46:da:ff:a1:1d:eb	d2:d9:a5:66:9e:12	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	6b:3d:98:85:ed:9a	b8:99:20:56:31:bc	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	f6:af:86:51:e4:59	22:e4:62:ff:56:e1	0.0.0.0	0.0.0.0	TCP	1	0.00
P3	8e:b0:27:e4:30:9b	51:e2:bb:ce:b4:0e	0.0.0.0	0.0.0.0	TCP	1	0.00
Others	Others	Others	Others	Others	Others	12474079	99.92
						Total: 12484080	

Others Total

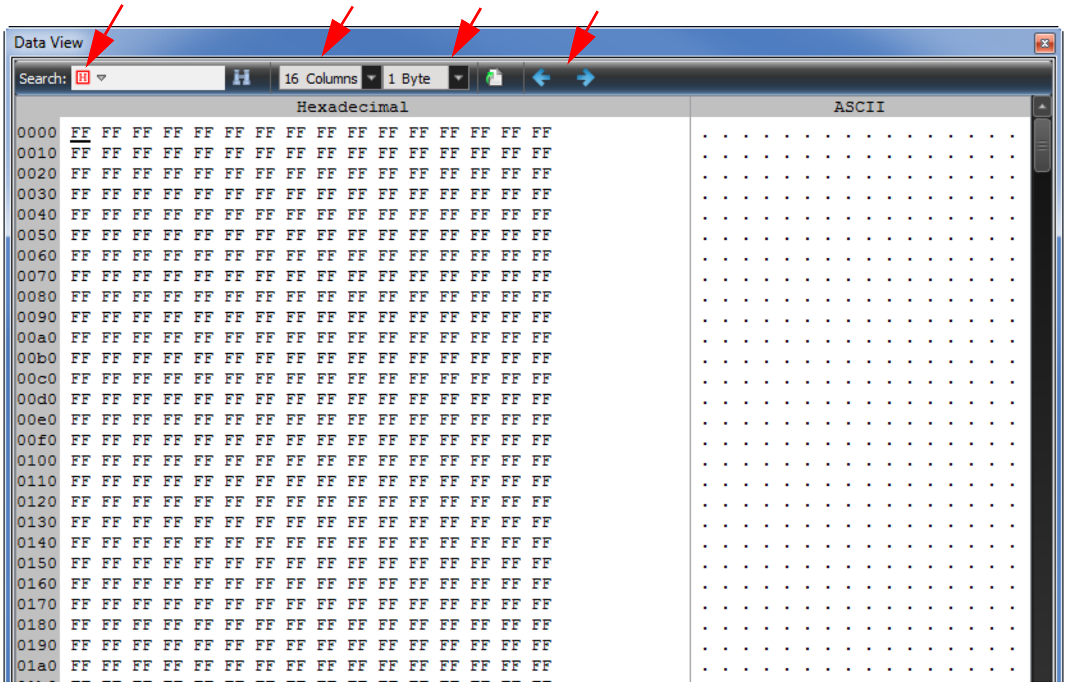
Figure 3.28: Source and Destination Columns in Traffic Summary View.

3.3.7 Data View

The Data View displays data in Hexadecimal and ASCII format (see Figure 3.29 on page 135). You can search for data by entering criteria in the Search field. Select an option from Columns and Bytes drop-down list to display the data. The formats available are:

- Columns: 1,2, 4, 8 and 16
- Bytes: 1,2, 4, 8 and 16

Click the **Export** button to display the Save Data Payload dialog to save the data.



```
0000 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0010 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0020 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0030 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0040 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0050 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0060 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0070 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0080 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0090 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
00a0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
00b0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
00c0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
00d0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
00e0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
00f0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0100 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0110 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0120 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0130 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0140 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0150 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0160 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0170 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0180 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
0190 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
01a0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ................
```

Figure 3.29: Data View

3.3.8 Customize Display

Ports

All active ports are highlighted on the Show/Hide Ports toolbar. Click the Ports button on the top toolbar to display the ports. Click a port button to hide the captured frames for that port. Frames can be displayed or hidden based on which port they were captured.

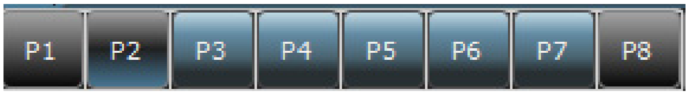


Figure 3.30: Show/Hide Ports Toolbar

Filter: Show/Hide Field

You can simplify the Viewer display by hiding packets. Click the Filter button on the top toolbar to Show/Hide packets and specify And/Or conditions as shown in Figure 3.30 on page 135 (see “Filtering” on page 138).

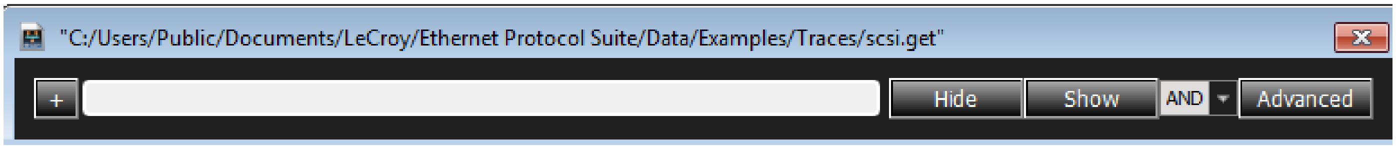

"C:/Users/Public/Documents/LeCroy/Ethernet Protocol Suite/Data/Examples/Traces/scsi.get"

Figure 3.31: Show/Hide Field

Note: Only the fields previously hidden appear in the restore list.

Show/Hide Idles

You can show or hide Idles by clicking on the Hide/Show Idles icon.

3.3.9 Toolbars

Enabling Tool Bars

To customize the Viewer Display workspace, you can enable and reposition the available toolbars. To display or hide toolbars, select **View > Toolbars**, then check or uncheck toolbars**.**

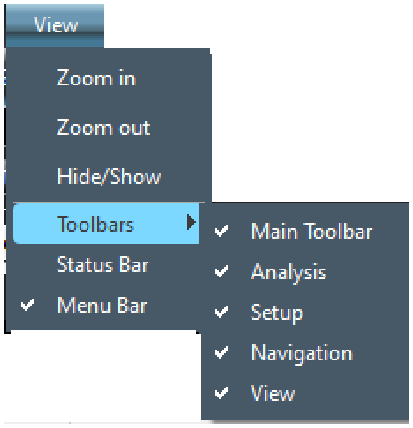


Figure 3.32: Customizing the Toolbar

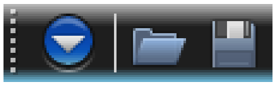
Toolbars are:

- Main
- Analysis
- Setup
- Navigation
- View

Once enabled, the toolbars can dock at the Viewer Display window or float on the windows desktop.

Main Toolbar

The Main or standard toolbar has the Hide Menubar, File Open and File Save. See “Software Menus and Toolbar” on page 36 for mor information.

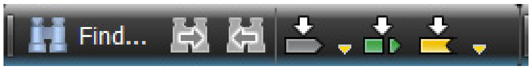


Analysis Toolbar

The Analysis toolbar displays various views. See “Switching Views” on page 117 for more information.

Navigation Toolbar

The Navigation toolbar allows searching, filtering, collapsing/expanding, and data reporting.



The **Find** button opens the **Find** dialog (see “Find” on page 144).

The **Find Next** button searches for the next matched packet or data previously set in the **Find** dialog (see “Find” on page 144).

The **Find Previous** button searches for the previous match packet or data previously set in the **Find** dialog (see “Find” on page 144).

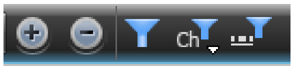
The down arrow on the **Go To** button allows location of cursors or specific packets: Trigger Position, X Position, Y Position, Timestamp, Event, Begin, and End.

The **Go to Trigger** goes to a trigger point.

The **Go to Marker** button opens the **Marker List** dialog (see “Markers” on page 127) and allows you to specify the marker to go to. The down arrow lists all the markers and you can select one to go to.

View Toolbar

The View toolbar allows wrapping, zooming, and configuration.



The **Zoom In** button on the View Toolbar magnifies the data display area on the screen. Clicking this button in Column or Text View increases column width only.

The **Zoom Out** button on the View Toolbar scales the data display area to display more data lines on the screen. Clicking this button in Column or Text View decreases column width only.

The **Filter** button on the View Toolbar opens the Filter dialog (see "Filtering" on page 138.)

The **Port Filters** button provides a popup that enables you to quickly filter traffic by port in the Spreadsheet View. See "Port Status Pane" on page 58.

The **Show/Hide Idles** button toggles between hiding and showing idles.

Setup Toolbar

The Setup toolbar is used to set preferences.

The **Preferences** button displays the Preferences dialog (see "Preferences" on page 40.)

3.3.10 Status Bar

The Status bar is located at the bottom of the main display window. Depending on the current activity, the bar can be divided into as many as four segments.

3.3.11 Search Status

The right most segment displays the current search direction: **Fwd** (forward) or **Bwd** (backward). Change the search direction from the Search Menu or double-click the Search Status segment.

3.4 Filtering

The Filtering menu and options allow you to modify data in the trace viewer display to exclude packets with a set of user-defined patterns and show the results in all views.

To set up filtering, you must have a viewer display open.

3.4.1 Filter Setup

To display the Quick Filter dialog (see Figure 3.33 on page 139), click the drop-down arrow of the **Filter** button on the toolbar or select **View > Hide/Show**. When Filter criteria are set, click the funnel icon on the Filter button to toggle the filters on and off.

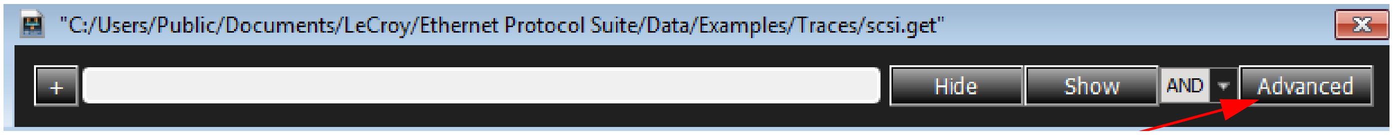

"C:/Users/Public/Documents/LeCroy/Ethernet Protocol Suite/Data/Examples/Traces/scsi.get"
+
Hide
Show
AND
Advanced

Figure 3.33: Quick Filter Dialog

You can Quick Search and Filter on a Frame by right-clicking on it in the trace and selecting **Quick Search**. Select a field to filter/search for. Click in between the two lines in the center to display logical operators to select from the drop-down list.

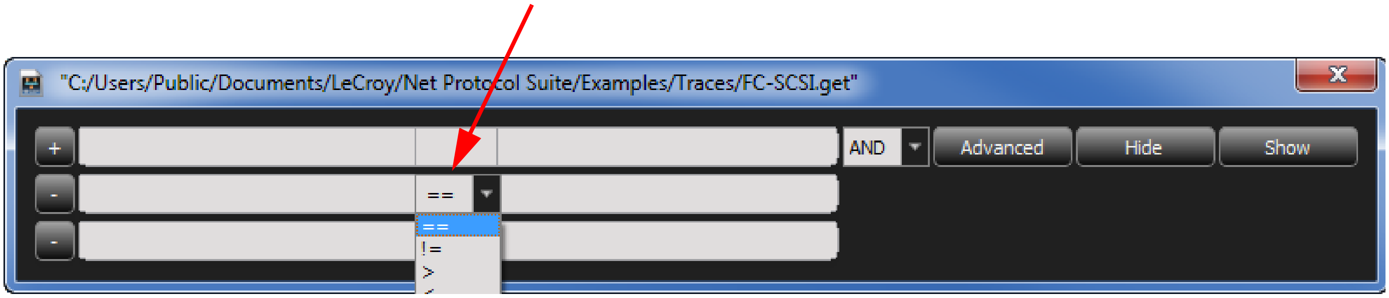

"C:/Users/Public/Documents/LeCroy/Net Protocol Suite/Examples/Traces/FC-SCSI.get"
+
-
-
==
==
!=
>
AND
Advanced
Hide
Show

Figure 3.34: Search/Quick Filter for Frame Dialog

Click the **Advanced** button (see Figure 3.33) on the Quick Filter dialog to display the Advanced Filter dialog (see Figure 3.35).

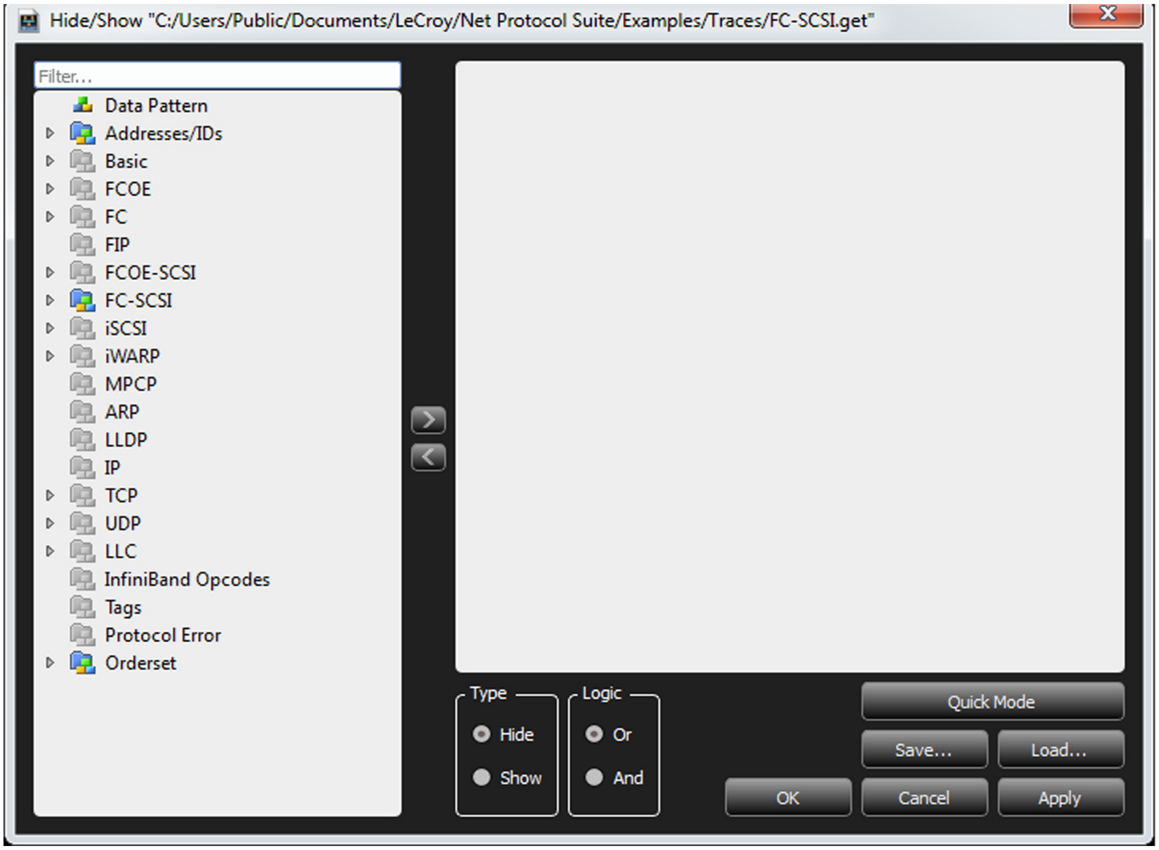


Figure 3.35: Advanced Filter Dialog

You can select or deselect each of the items shown in the left pane for filtering. Items not in the current trace are greyed out.

NOTE 1: If you select a group, that also selects all child items.

NOTE 2: Only packets captured at run time are available for selection for filtering.

Filter Type

You can choose to show or hide the Filter Type items by checking the Show or Hide option button.

Filter Logic

After you have set up Filter options, you can set filter logic to **And** to apply “AND” logic on related selected options or **OR** to apply “OR” logic on all selected options.

Save Filter

After you have set up a Filter configuration, you can save it as a Filter file by clicking **Save**.

Load

You can use a previously saved filter by clicking **Load** in the Filter dialog.

Apply

You can apply the current filter by clicking **Apply** in the Filter dialog.

Filtering LUNs and LBAs

Perform the following steps to filter for LUNs and LBAs:

1. Click the drop-down arrow of the **Filter** button to display the Quick Filter dialog.
2. Click **Advanced** to display the Hide/Show dialog.
3. Select FCP_CMD in the left pane and drag it in to the right pane or click the right arrow.

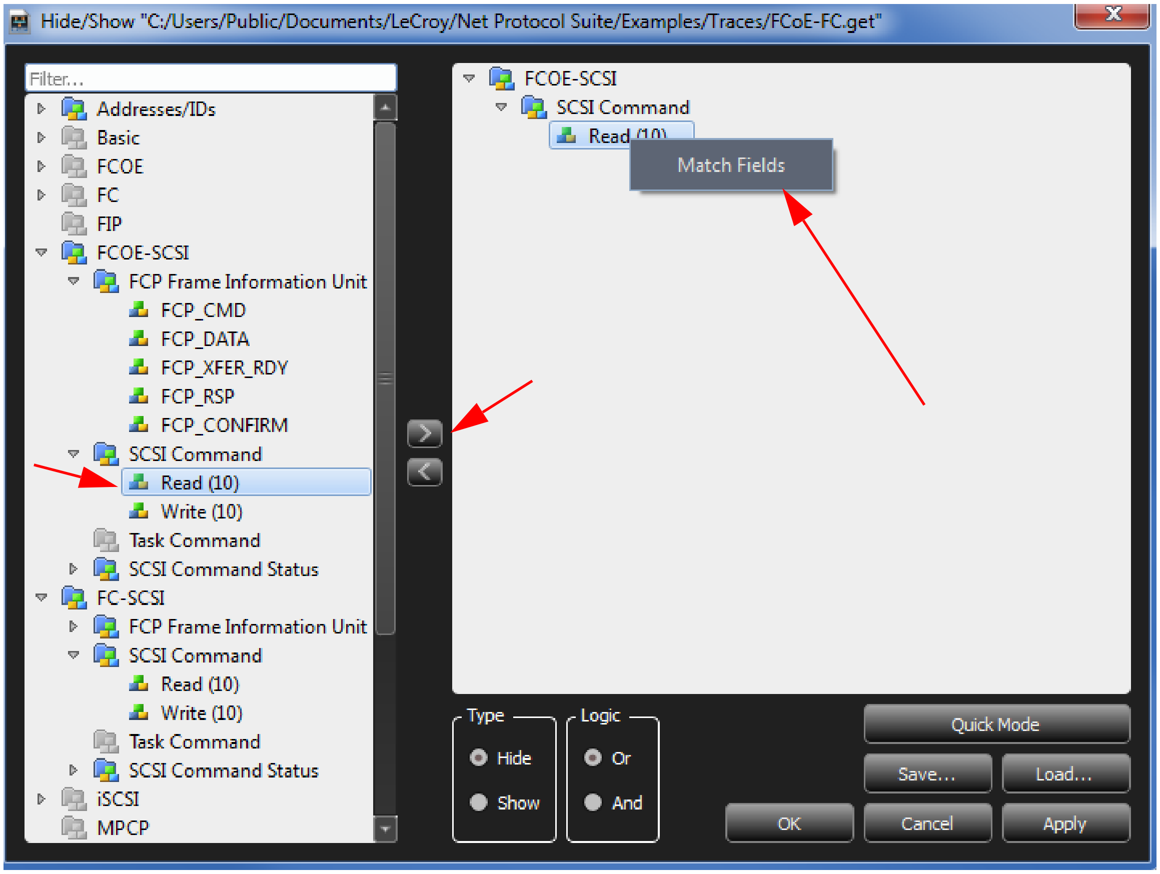
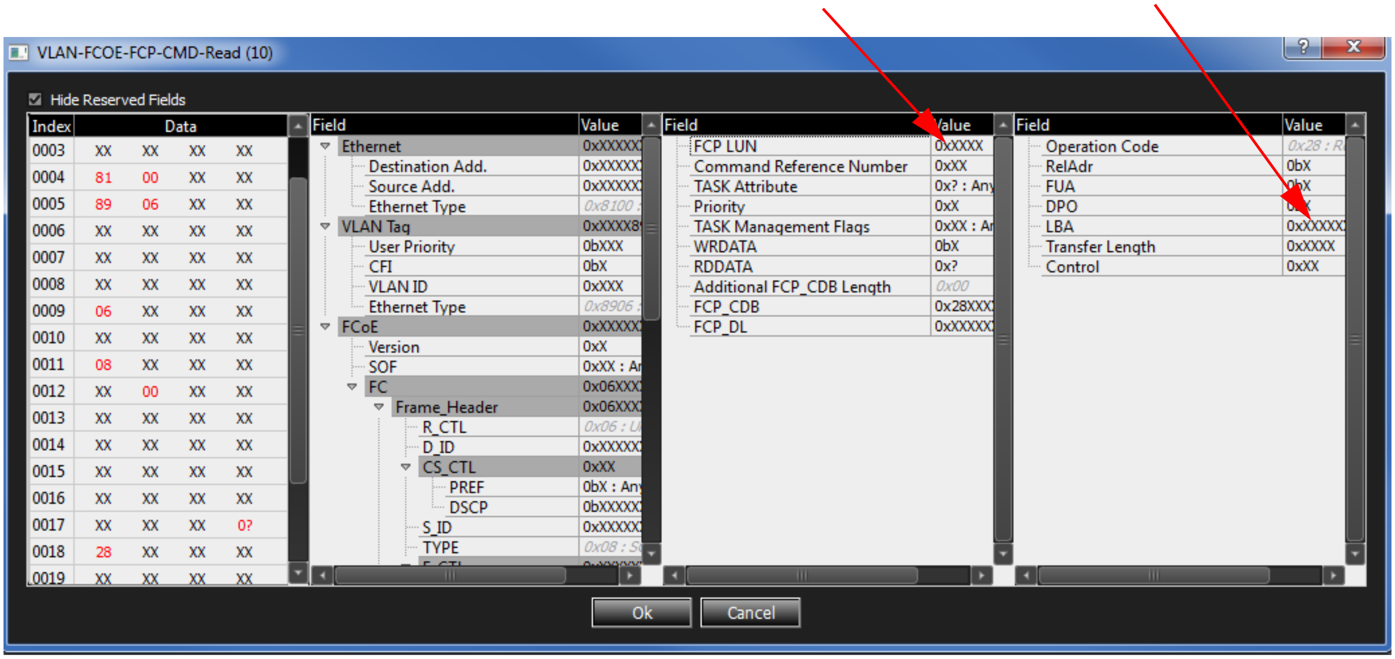


Figure 3.36: Filtering for LUNs and LBAs

4. Select the command, double-click or right-click, and select **Match Fields**. The following filter dialog displays (see Figure 3.35 on page 140).
5. Enter the values in the field.
6. Click **OK** twice.



☑ Hide Reserved Fields

Index	Data			
0003	XX	XX	XX	XX
0004	81	00	XX	XX
0005	89	06	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	06	XX	XX	XX
0010	XX	XX	XX	XX
0011	08	XX	XX	XX
0012	XX	00	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX
0015	XX	XX	XX	XX
0016	XX	XX	XX	XX
0017	XX	XX	XX	0?
0018	28	XX	XX	XX
0019	XX	XX	XX	XX

Field	Value
Ethernet	0xXXXXX
Destination Add.	0xXXXXX
Source Add.	0xXXXXX
Ethernet Type	0x8100 :
VLAN Tag	0xXXXX8
User Priority	0bXXX
CFI	0bX
VLAN ID	0xXXX
Ethernet Type	0x8906 :
FCoE	0xXXXXX
Version	0xX
SOF	0xXX : Ar
FC	0x06XXX
Frame_Header	0x06XXX
R_CTL	0x06 : U
D_ID	0xXXXXX
CS_CTL	0xXX
PREF	0bX : Any
DSCP	0bXXXXX
S_ID	0xXXXXX
TYPE	0x08 : S

Field	Value
FCP LUN	0xXXXX
Command Reference Number	0xXX
TASK Attribute	0x? : Any
Priority	0xX
TASK Management Flags	0xXX : Ar
WRDATA	0bX
RDDATA	0x?
Additional FCP_CDB Length	0x00
FCP_CDB	0x28XXX
FCP_DL	0xXXXXX

Field	Value
Operation Code	0x28 : R
RelAdr	0bX
FUA	0bX
DPO	0bX
LBA	0xXXXXX
Transfer Length	0xXXXX
Control	0xXX

Figure 3.37: LUN and LBA Filter

3.5 Using Cursors

3.5.1 Cursors

The spreadsheet view display incorporates three cursors labeled **X, Y,** and **T.** All cursors are initially overlaid and positioned at location 0, which is the trigger position of the display. The Trigger, or **T**, cursor is the measurement reference and is always at location 0 in the display.

Positioning the X Cursor

To position the X-Cursor within the viewer data display, click the left mouse button in the gray bar on the left side of the trace viewer next to the line in which to place the cursor.

Positioning the Y Cursor

To position the Y-cursor within the viewer data display, click the right mouse button in the gray bar on the left side of the trace viewer next to the line in which to place the cursor.

Locate Cursors

To quickly locate any cursor within the data viewer display, right-click and select the **Go To X** or **Go To Y** option and choose the cursor to locate (see Figure 3.38 on page 143). You can also locate a cursor by selecting **Go To** from the Navigation menu and choosing the cursor to locate.

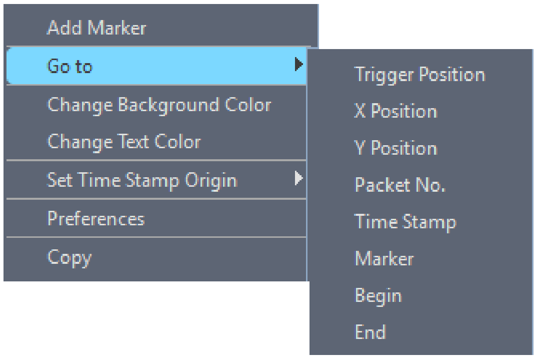


Figure 3.38: Locate Cursor

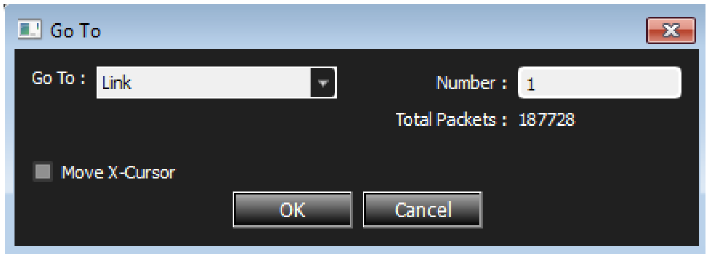
Go to Trigger

Moves the view to the Trigger.

Go to Packet/Event

To locate a packet, select **Go To Event** or right-click and choose **Packet**.

Enter a Link or Sequence value and number in the Go To dialog and click **OK**.



Go To : Link

Number : 1

Total Packets : 187728

□ Move X-Cursor

Figure 3.39: Go to Dialog

Go to Begin

To go to the beginning of a trace, click the **Go To** button or right-click and choose **Begin**.

Go to End

To go to the end of a trace, click the **Go To** button or right-click and choose **End**.

Set Time Stamp Origin

Right-click and choose **Set Time Stamp Origin** (see Figure 3.40 on page 144). For details see “Spreadsheet View Menu Options” on page 122.

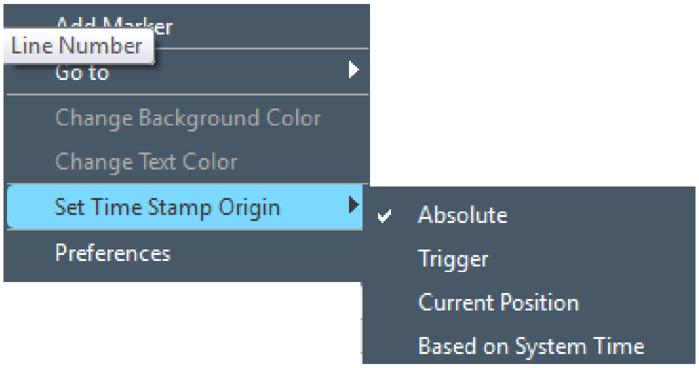
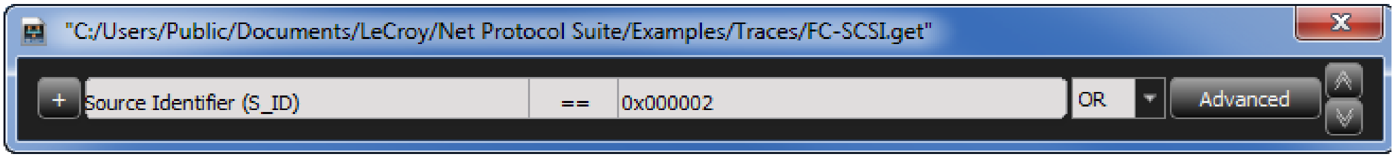


Figure 3.40: Set Time Stamp Dialog

3.6 Find

The Find menu and toolbar options permit you to examine any data capture file to quickly locate the packet or data pattern. Select **Navigation> Find** or click the **Find** button to open the **Quick Find** dialog (see Figure 3.41 on page 144). You can also right-click in the trace and select **Quick Search**.

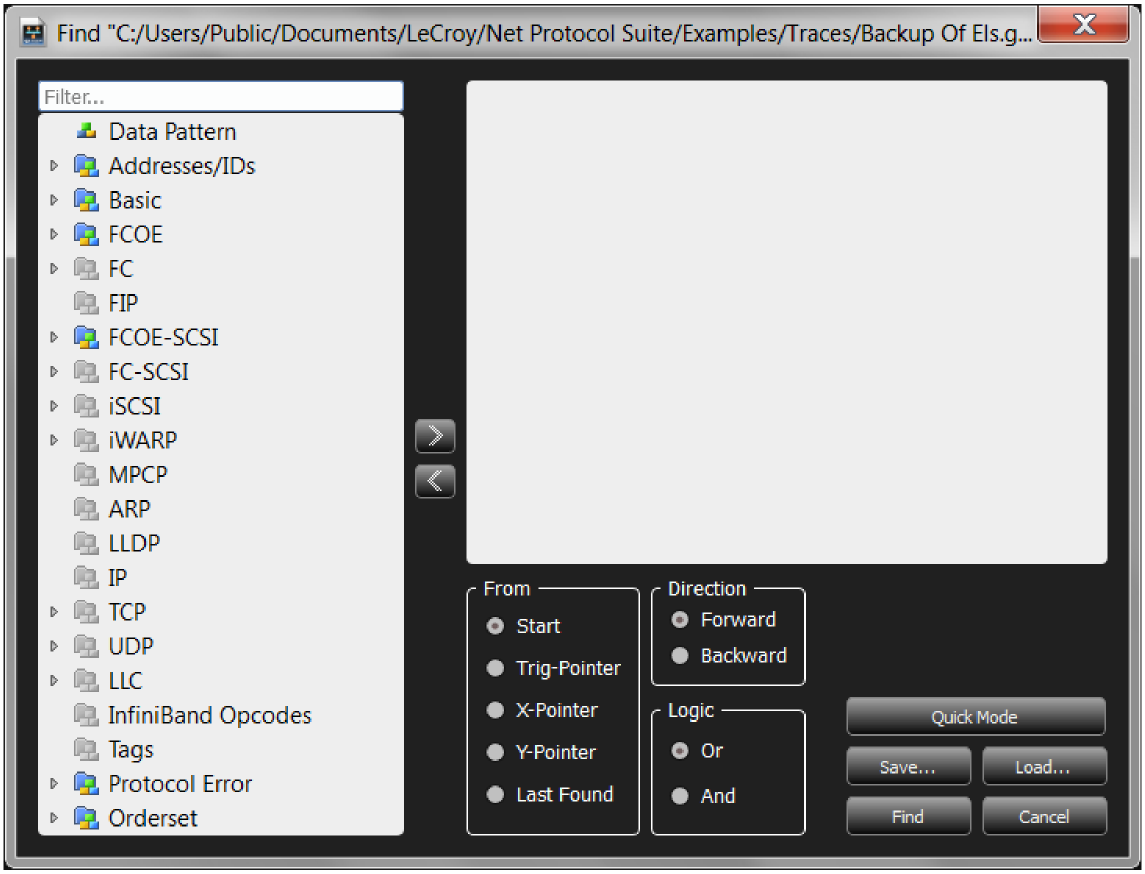
Note: Only items captured in the trace file are enabled for search.


"C:/Users/Public/Documents/LeCroy/Net Protocol Suite/Examples/Traces/FC-SCSI.get"

Source Identifier (S_ID) == 0x000002 OR

Figure 3.41: Quick Find Dialog

Click the **Advanced** button on the Quick Find dialog to display the Advanced Find dialog (see Figure 3.42 on page 145).



Find "C:/Users/Public/Documents/LeCroy/Net Protocol Suite/Examples/Traces/Backup Of Els.g...

From: ◉ Start ○ Trig-Pointer ○ X-Pointer ○ Y-Pointer ○ Last Found

Direction: ◉ Forward ○ Backward

Logic: ◉ Or ○ And

Figure 3.42: Advanced Find Dialog

Save

After you have set up a Filter configuration, you can save it as a Filter file by clicking **Save**.

Load

You can use a previously saved filter by clicking **Load** in the Filter dialog.

Find

You can find specific packets by selecting one and clicking **find** in the Filter dialog.

You can continue to search the output file using **Find Next (F3)** or **Find Previous (F4)** for the same pattern, until you redefine the data capture search parameters. You can also click the **Find Next** icon or the **Find Previous** icon. Alternatively, select **Navigation > Find Next** or **Navigation > Find Previous**.

3.6.1 Save Find Setup

After you have set up a Find configuration, you can save it as a Search configuration file by clicking **Save**. You can then use it on a different capture by clicking **Load** in the Find dialog.

3.6.2 Search From

Choose a starting point to begin or continue a search: Start of the trace file, Trigger Pointer, X Pointer, Y Pointer, or Last Found.

3.6.3 Find Direction

Choose either **Forward** or **Backward** direction in which to perform the find.

3.6.4 Find Logic

The default setting is **Or**. With this setting, clicking **Find Next** locates all selected items in turn. If you choose **And,** you can set a logical AND combination of items to find. Both options allow setting Advanced find features.

3.6.5 Finding LUNs and LBAs

Perform the following steps to find LUNs and LBAs:

1. Click the **Find** icon to display the Quick Find dialog.
2. Click **Advanced** to display the Find dialog.
3. Select FCP_CMD in the left pane and drag it in to the right pane or click the right arrow.

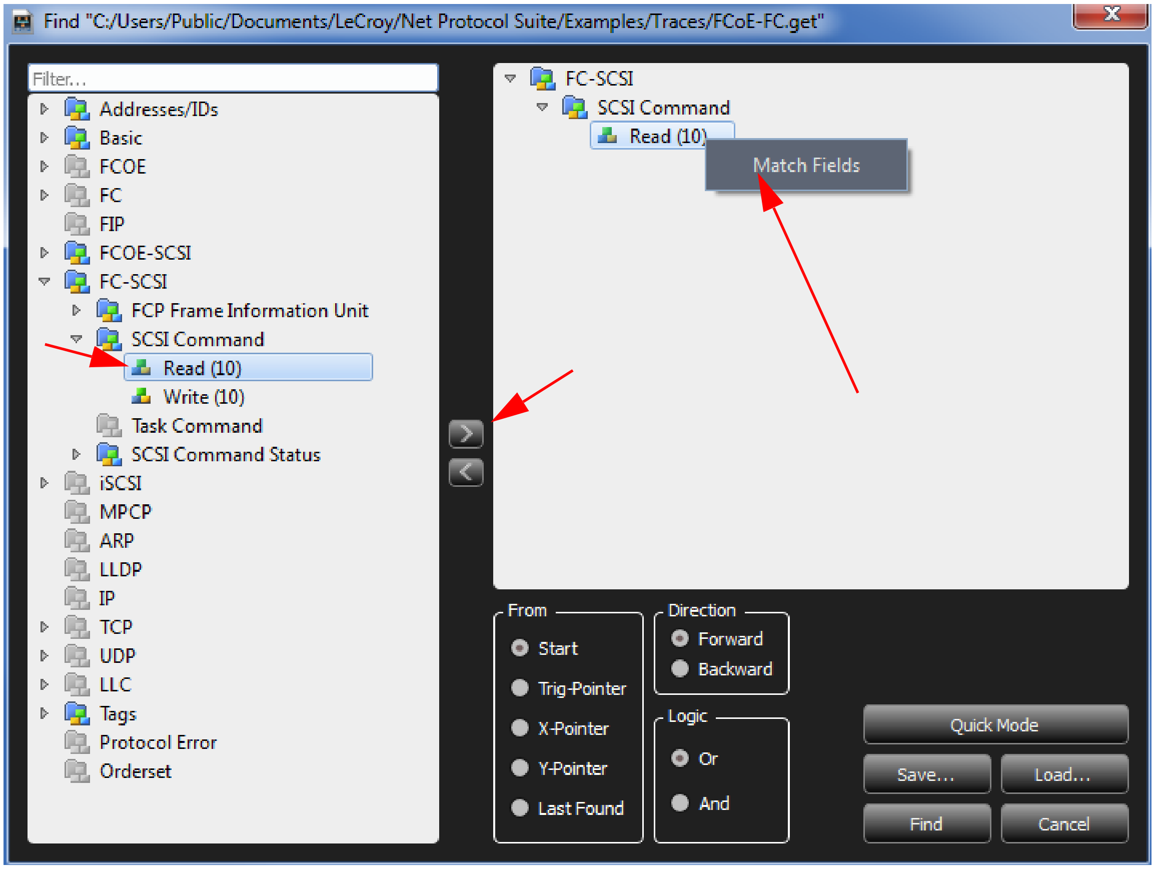
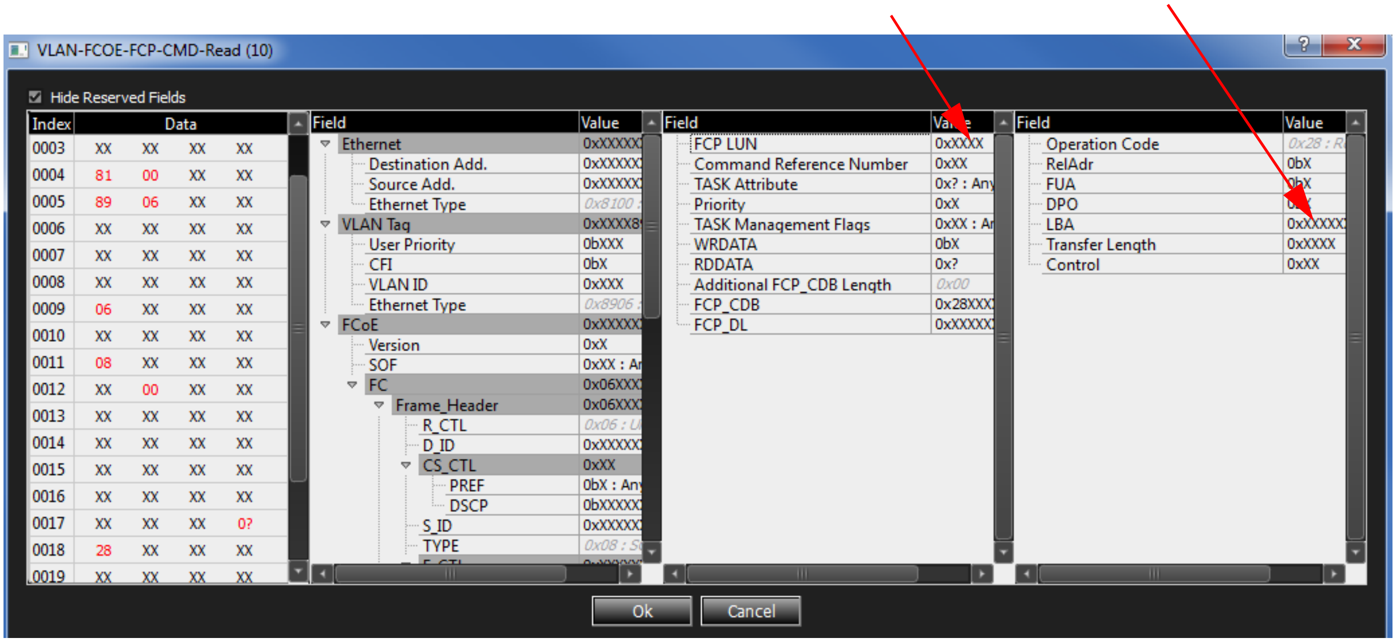

Find "C:/Users/Public/Documents/LeCroy/Net Protocol Suite/Examples/Traces/FCoE-FC.get"

Figure 3.43: Find LUNs and LBAs 1

4. Select the command, double-click or right-click, and select **Match Fields**. The following dialog displays (see Figure 3.44).
5. Enter the values in the fields.
6. Click **OK** twice.



VLAN-FCOE-FCP-CMD-Read (10)

☑ Hide Reserved Fields

Index	Data			
0003	XX	XX	XX	XX
0004	81	00	XX	XX
0005	89	06	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	06	XX	XX	XX
0010	XX	XX	XX	XX
0011	08	XX	XX	XX
0012	XX	00	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX
0015	XX	XX	XX	XX
0016	XX	XX	XX	XX
0017	XX	XX	XX	0?
0018	28	XX	XX	XX
0019	XX	XX	XX	XX

Field	Value
Ethernet	0xXXXXX
Destination Add.	0xXXXXX
Source Add.	0xXXXXX
Ethernet Type	0x8100 :
VLAN Tag	0xXXXX8
User Priority	0bXXX
CFI	0bX
VLAN ID	0xXXX
Ethernet Type	0x8906 :
FCoE	0xXXXXX
Version	0xX
SOF	0xXX : A
FC	0x06XXX
Frame_Header	0x06XXX
R_CTL	0x06 : U
D_ID	0xXXXXX
CS_CTL	0xXX
PREF	0bX : An
DSCP	0bXXXXX
S_ID	0xXXXXX
TYPE	0x08 : S

Field	Value
FCP LUN	0xXXXX
Command Reference Number	0xXX
TASK Attribute	0x? : Any
Priority	0xX
TASK Management Flags	0xXX : A
WRDATA	0bX
RDDATA	0x?
Additional FCP_CDB Length	0x00
FCP_CDB	0x28XXX
FCP_DL	0xXXXXX

Field	Value
Operation Code	0x28 : R
RelAdr	0bX
FUA	0bX
DPO	0bX
LBA	0xXXXXX
Transfer Length	0xXXXX
Control	0xXX

Figure 3.44: Find LUNs and LBAs 2

3.6.6 Data Pattern Search

From the Advanced Find/Filter dialog, there is a Data Pattern item available (see Figure 3.45 on page 148).

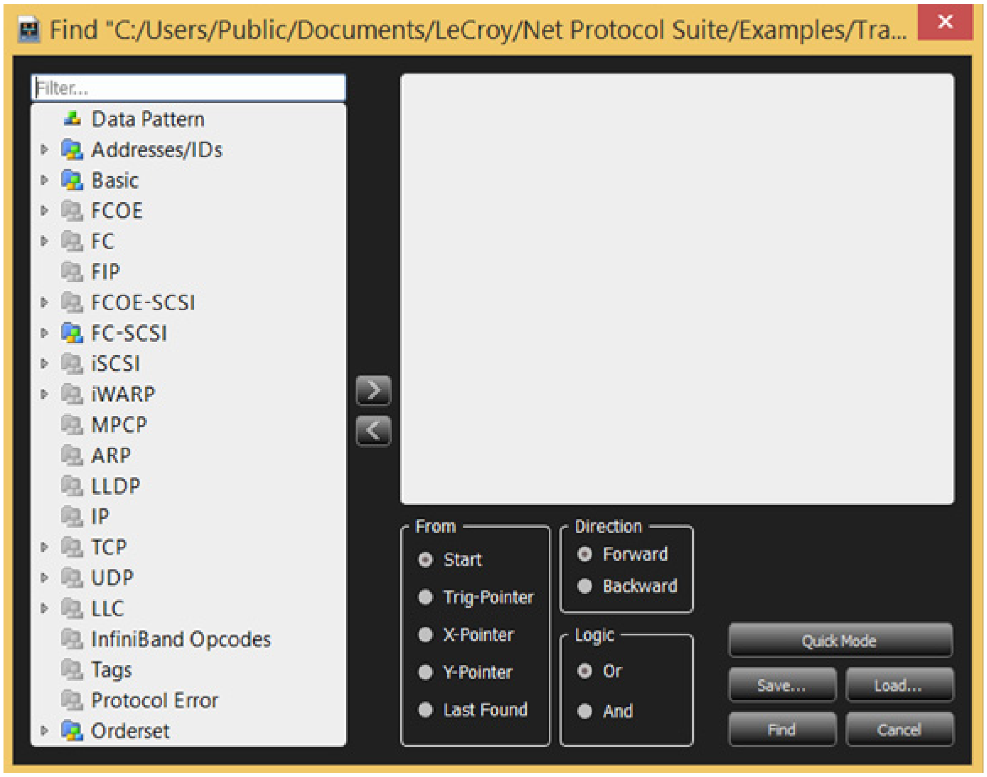


Figure 3.45: Data Pattern Search Menu

You may use this feature to set criteria based on Data Patterns in the frame payloads.

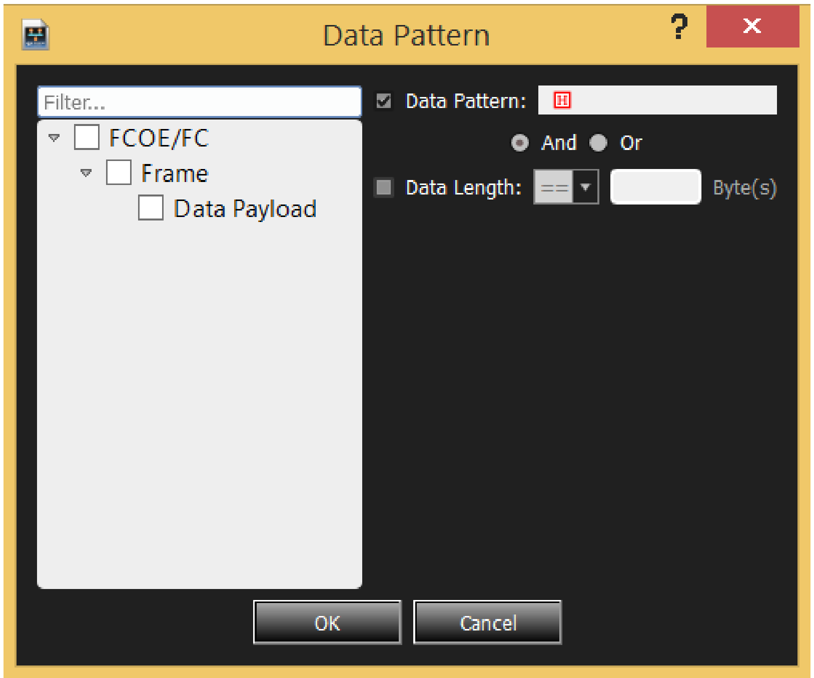


Figure 3.46: Data Pattern Search Filter

1. From the tree list on the left, select the types of payloads you want to search/filter against.
2. Check the boxes next to 'Data Pattern' and 'Data Length' to set whether you check based on those criteria or not.
3. If you check both the 'Data Pattern' and 'Data Length' boxes, also select the And/Or radio button to set whether you want to combine the criteria with AND or OR logic.
4. If 'Data Pattern' is checked, enter the pattern you wish to match against. You may specify any size of pattern in this field. Click the red format button to toggle between different input format modes:

    a. Hex

    b. Binary

    c. ASCII

    d. Decimal

5. If 'Data Length' is checked, enter the length in bytes you wish to match against, and set the desired comparison operator:

    a. == (equal)

    b. != (not equal)

    c. > (greater than)

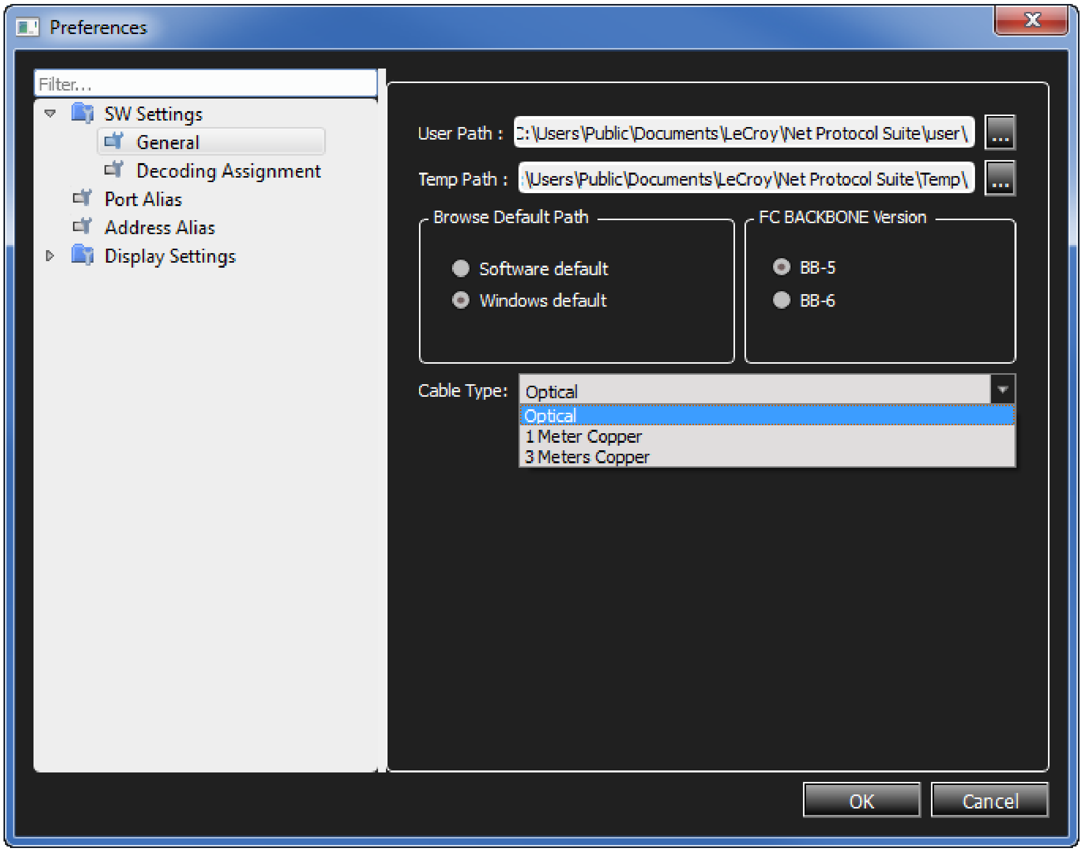
    d. < (less than)

    e. >= (greater than or equal)

    f. <= (less than or equal)

3.7 Preferences

The Analyzer ships with a default configuration for software settings, port alias, address alias, display and sequencer settings. You can define your own settings for a particular testing scenario. To set these preferences select **Setup** > **Preferences** or click the icon on the main toolbar to display the Preferences dialog (see Figure 3.47 on page 150).



Preferences

Filter...

User Path : C:\Users\Public\Documents\LeCroy\Net Protocol Suite\user\ ...

Temp Path : \Users\Public\Documents\LeCroy\Net Protocol Suite\Temp\ ...

Browse Default Path

○ Software default

● Windows default

FC BACKBONE Version

● BB-5

○ BB-6

Cable Type: Optical

Figure 3.47: Preferences Dialog

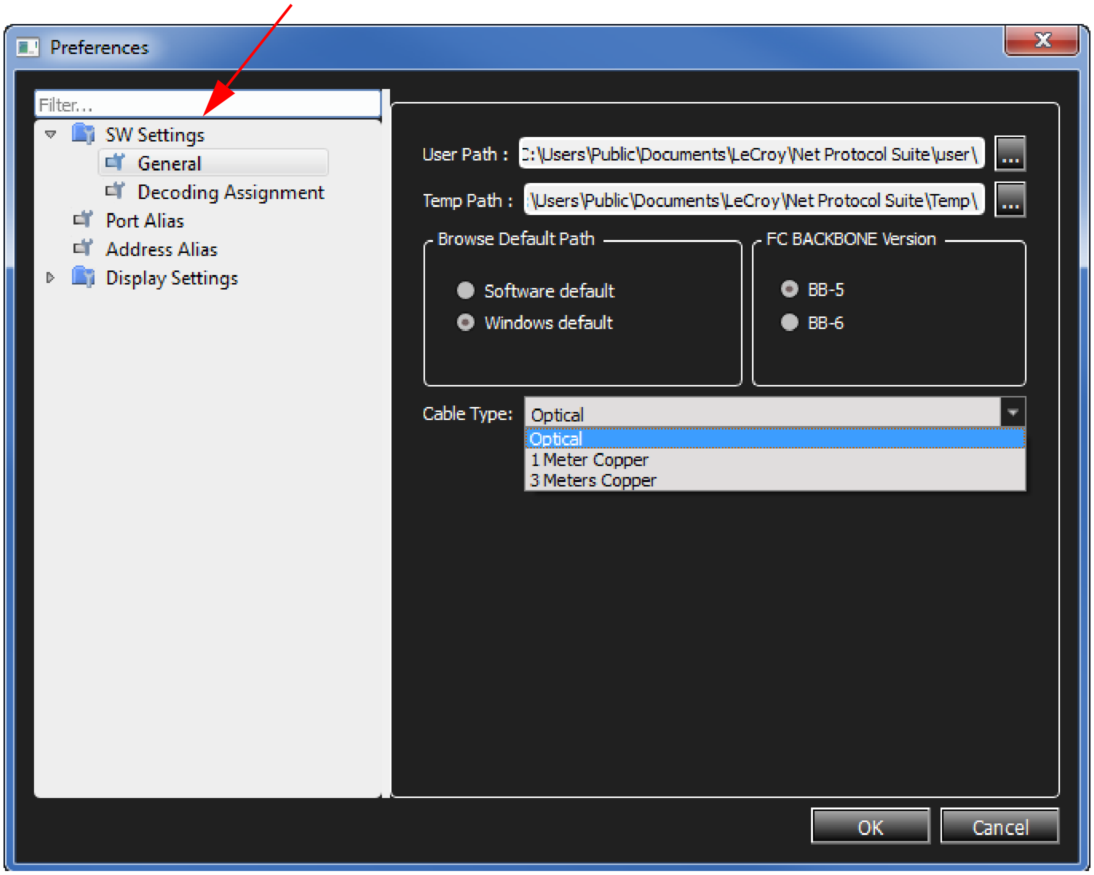
3.7.1 Software Settings

Software Settings allow you to define template files for new Analyzer projects, to specify how trace files appear when opened, and to set Spec Assignment.

In General you can select the User Path and Temp path by clicking the ... icon or browse to one of the default paths which are Software default and Windows default. See the figure below.

Select BB-5 or BB-6 for the FC BACKBONE Version.

Select Cable Type from the drop-down list.



User Path : C:\Users\Public\Documents\LeCroy\Net Protocol Suite\user\

Temp Path : \Users\Public\Documents\LeCroy\Net Protocol Suite\Temp\

Browse Default Path

○ Software default

● Windows default

FC BACKBONE Version

● BB-5

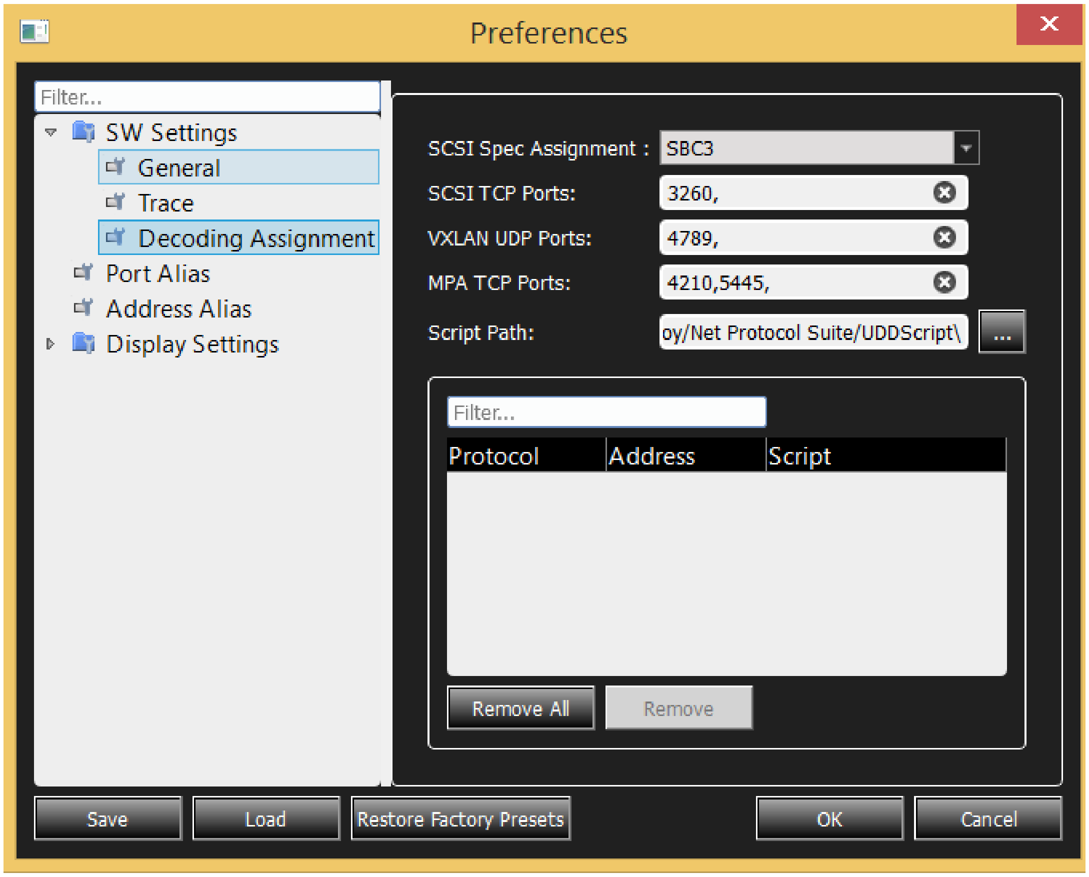
○ BB-6

Cable Type: Optical

- Optical
- 1 Meter Copper
- 3 Meters Copper

Figure 3.48: Software Settings General Options

Decoding Assignments



SCSI Spec Assignment : SBC3

SCSI TCP Ports: 3260,

VXLAN UDP Ports: 4789,

MPA TCP Ports: 4210,5445,

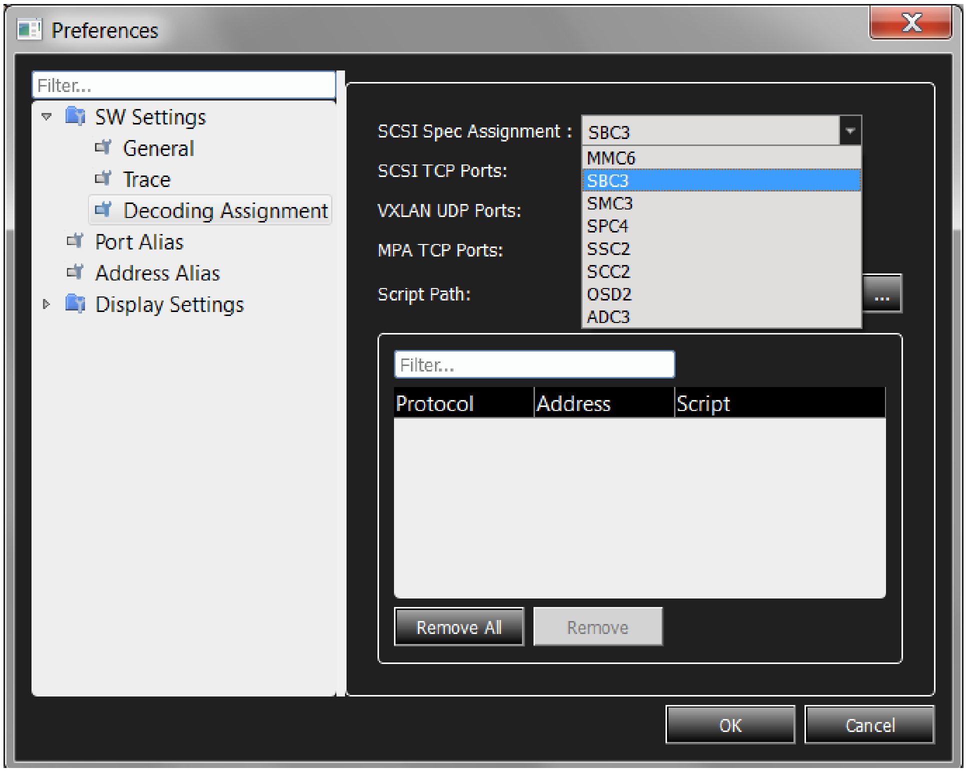
Script Path: oy/Net Protocol Suite/UDDScript\

Figure 3.49: Decoding Assignments

These settings enable you to customize which protocol decoders are applied to the data in captured traces. Settings made here will apply to subsequent traces that are created. To apply new settings to an existing trace, first set the settings as desired, then open the trace, select File -> Save As and save the trace to a new file. The new file will have the new decoding assignment settings applied.

- SCSI Spec Assignment: Select which SCSI command set to apply for decoding of SCSI commands.
- SCSI TCP Ports: Set which TCP ports are assigned for the iSCSI protocol.
- VXLAN UDP Ports: Set which UDP ports are assigned for the VXLAN protocol.
- MPA TCP Ports: Set which TCP ports are assigned for the MPA protocol.
- Script Path: Set the base script directory used for looking up user-defined decoding scripts. Refer to “Decoding Assignments” on page 117 for details on assigning script decoders.
- For the Ports settings, you may specify a list of ports by separating port numbers with commas (e.g., "400, 403, 407"). You may specify a range of ports by using a hyphen between the lower and upper port numbers of the range (e.g., "1200-1207").

The Decoding Assignments allow the user to configure SCSI command set assignments (see “SCSI Spec Assignments” on page 153), well-known port numbers assignments, and decoding script assignments.

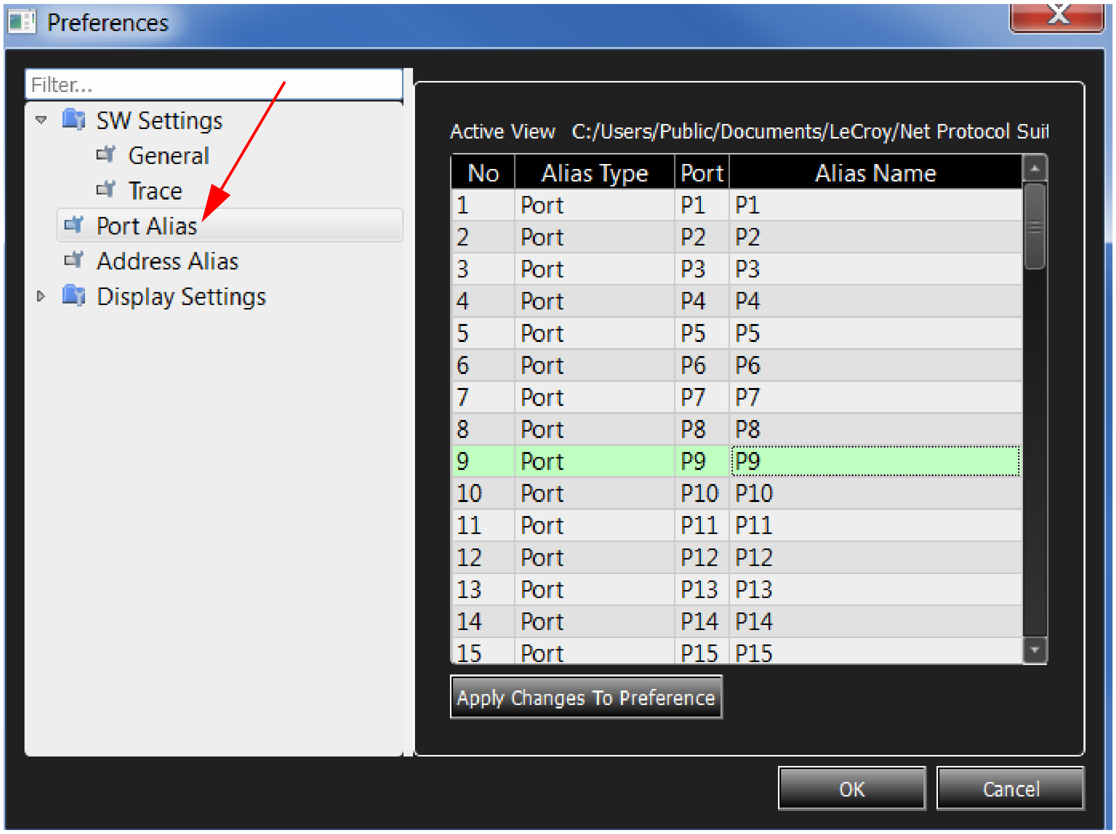


SCSI Spec Assignment : SBC3

Figure 3.50: SCSI Spec Assignments

3.7.2 Port Alias

Port Alias allows you to assign a meaningful name to each port to assist in interpreting the results displayed in the trace view. You can set the alias name for each port. Double click an Alias Name and enter a name. See the figure below.



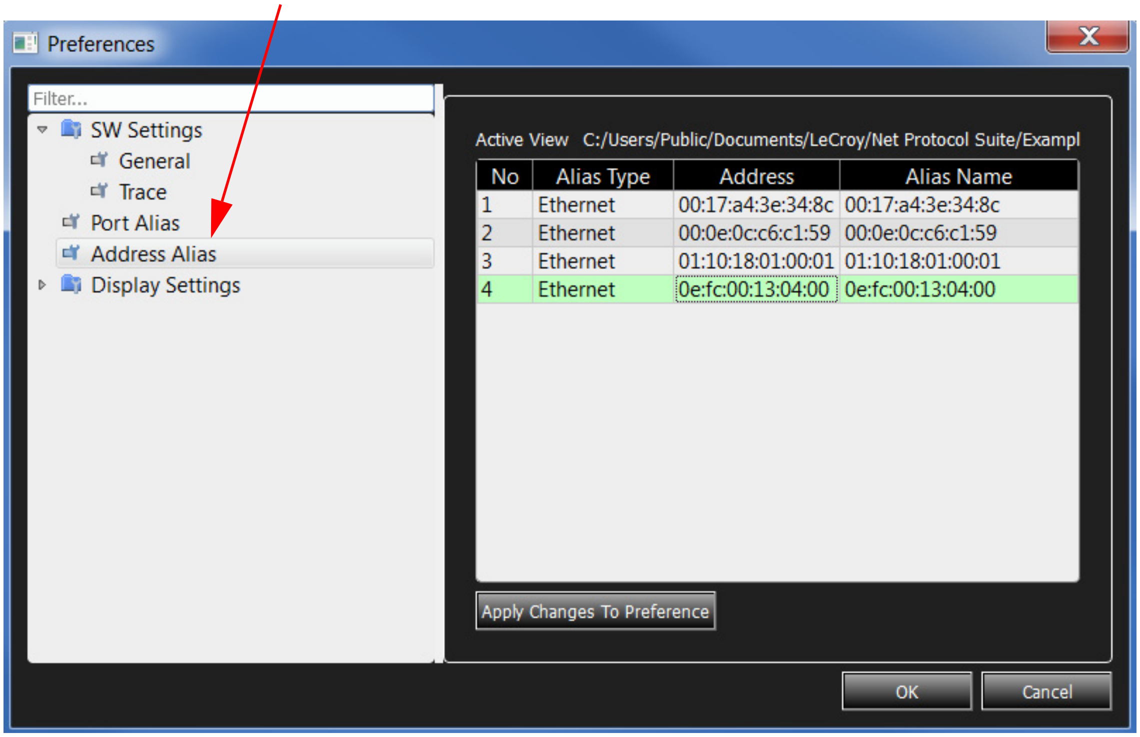
Active View C:/Users/Public/Documents/LeCroy/Net Protocol Suit

No	Alias Type	Port	Alias Name
1	Port	P1	P1
2	Port	P2	P2
3	Port	P3	P3
4	Port	P4	P4
5	Port	P5	P5
6	Port	P6	P6
7	Port	P7	P7
8	Port	P8	P8
9	Port	P9	P9
10	Port	P10	P10
11	Port	P11	P11
12	Port	P12	P12
13	Port	P13	P13
14	Port	P14	P14
15	Port	P15	P15

Figure 3.51: Port Alias Dialog

3.7.3 Address Alias

Address Alias allows you to assign a meaningful name to each address to assist in interpreting the results displayed in the trace view You can set the alias name for each address. Double click an Alias Name and enter a name. See the figure below.



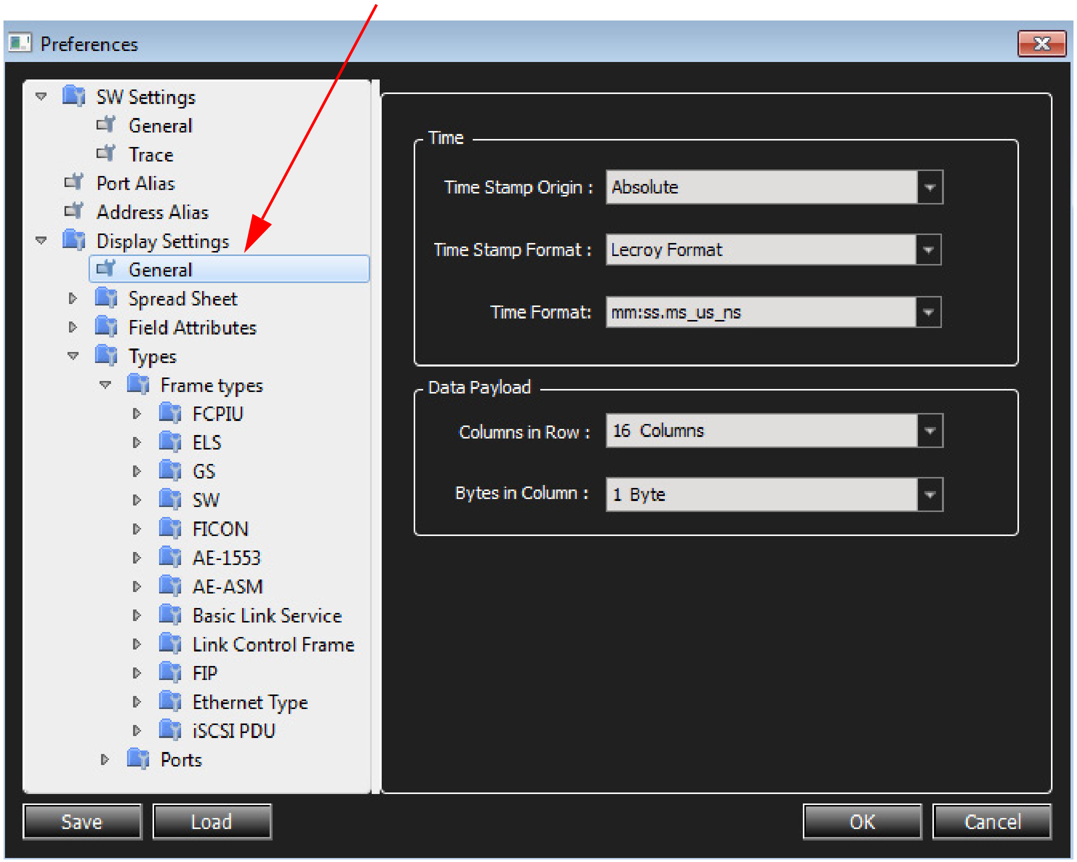
Active View C:/Users/Public/Documents/LeCroy/Net Protocol Suite/Exampl

No	Alias Type	Address	Alias Name
1	Ethernet	00:17:a4:3e:34:8c	00:17:a4:3e:34:8c
2	Ethernet	00:0e:0c:c6:c1:59	00:0e:0c:c6:c1:59
3	Ethernet	01:10:18:01:00:01	01:10:18:01:00:01
4	Ethernet	0e:fc:00:13:04:00	0e:fc:00:13:04:00

Figure 3.52: Address Alias Dialog

3.7.4 Display Settings

In General you can select the Time options and the Data Payload options from the drop-down lists. See the figure below.



Time

Time Stamp Origin : Absolute

Time Stamp Format : Lecroy Format

Time Format: mm:ss.ms_us_ns

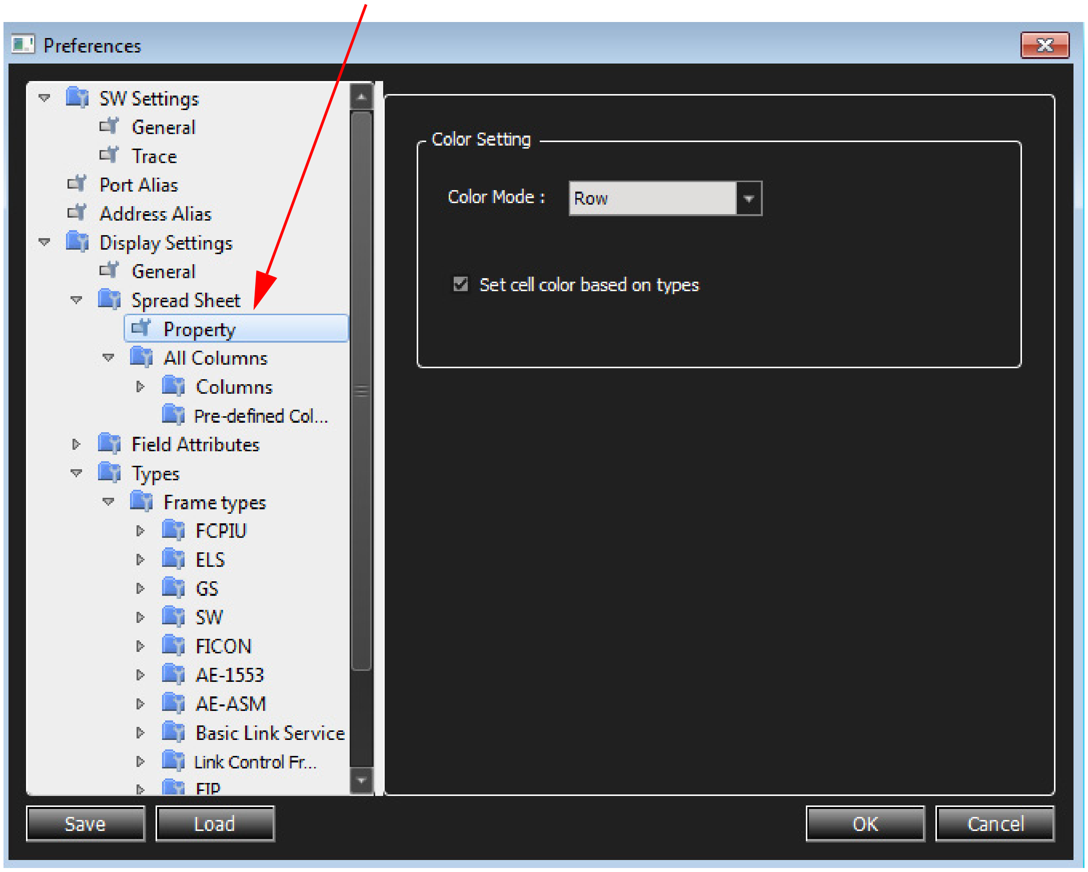
Data Payload

Columns in Row : 16 Columns

Bytes in Column : 1 Byte

Figure 3.53: Display Settings General Dialog

In Spreadsheet you can click **Property** and select the Color Setting option for row and column from the drop-down list. See the figure below.

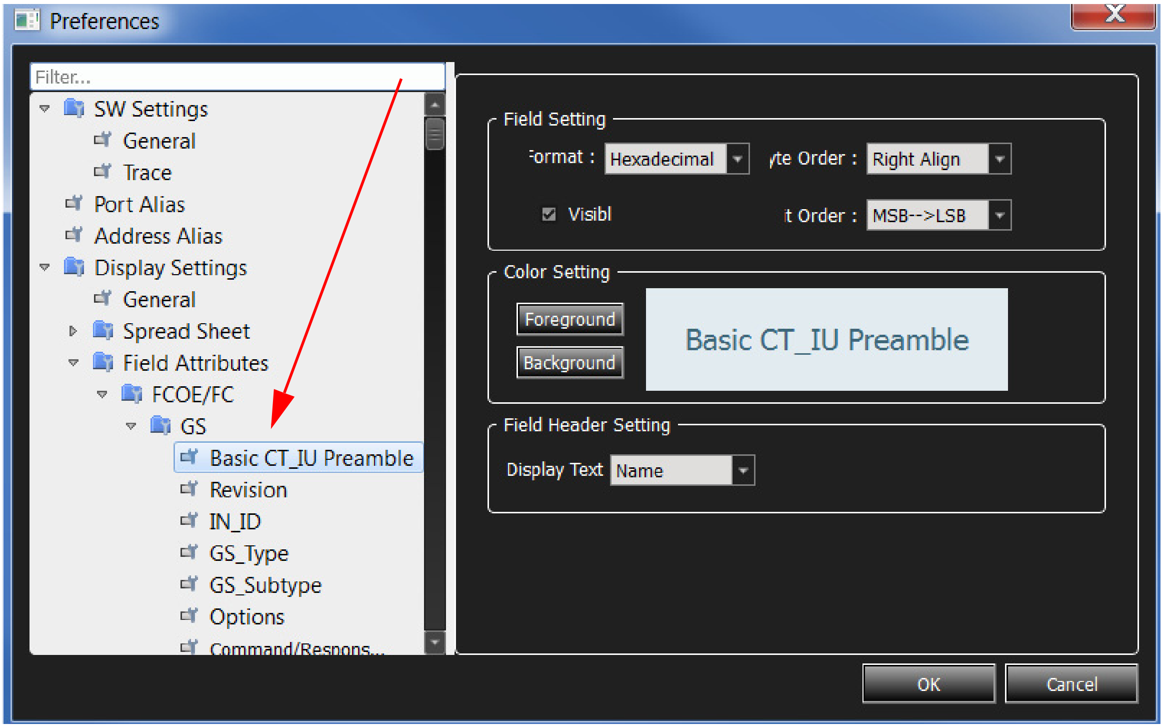


Color Mode : Row

☑ Set cell color based on types

Figure 3.54: Display Settings Spreadsheet Dialog

In Field Attributes you can click a **Trigger Pattern** and select the, Field Setting, Color Setting and Field Header Setting options from the drop-down lists. See the figure below.



ormat : Hexadecimal

yte Order : Right Align

☑ Visibl

t Order : MSB-->LSB

Display Text Name

Figure 3.55: Display Settings Field Attributes Dialog

In Frame types you can select the foreground and background Color Setting by clicking on the relevant button. See the figure below.

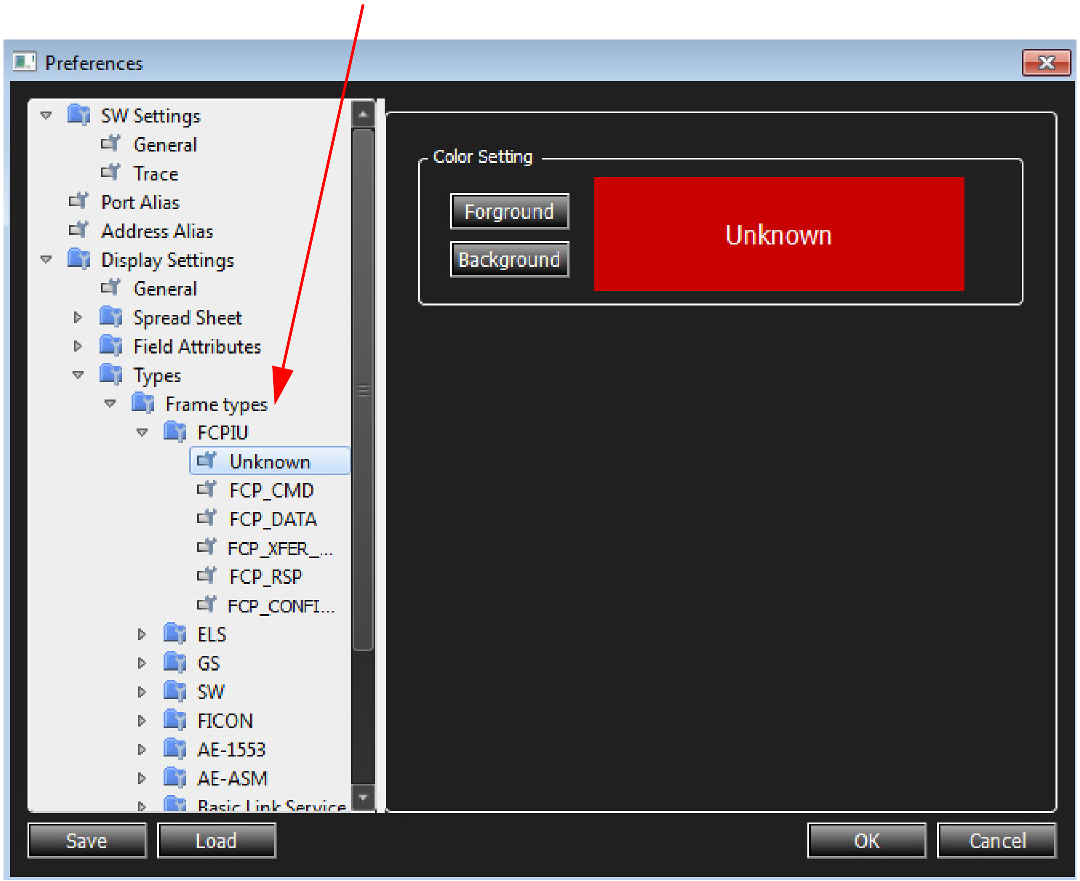


Figure 3.56: Display Settings Frame Types Dialog

In Ports you can select the foreground and background Color Setting by clicking on he relevant button. See Figure 3.56 on page 159.

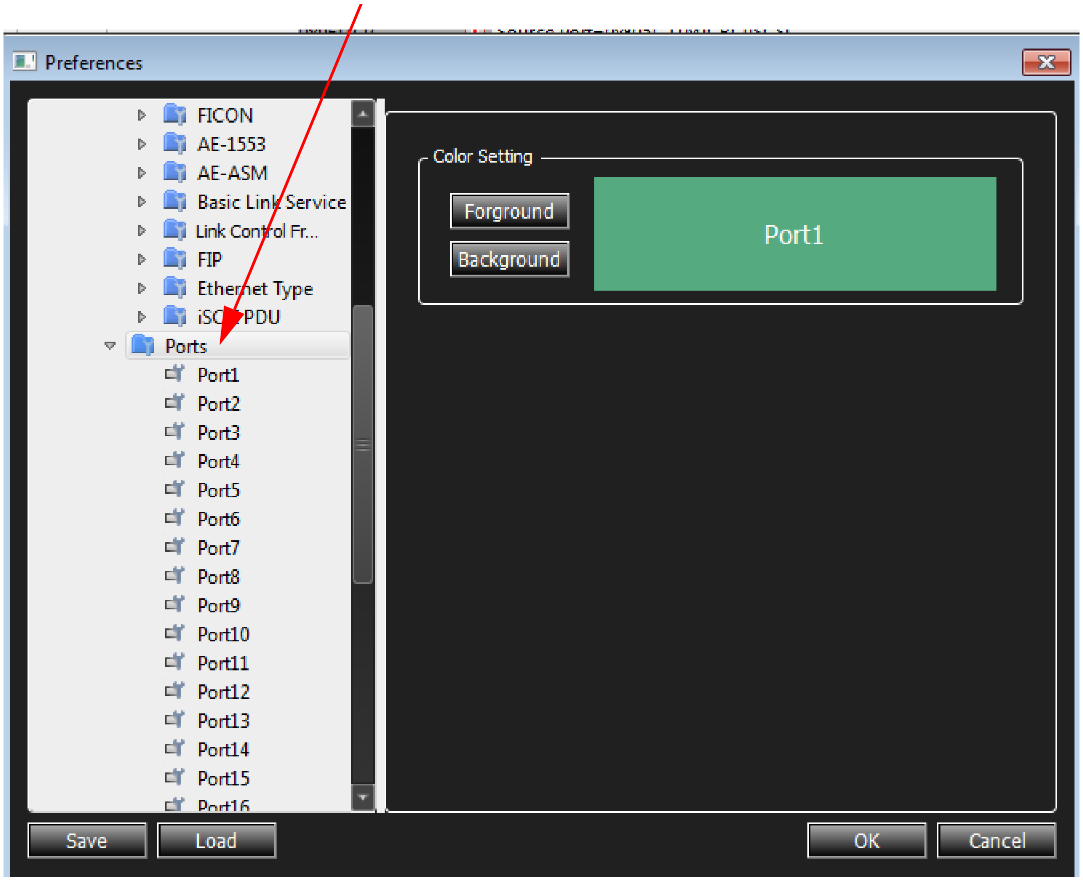


Figure 3.57: Display Settings Ports Dialog

3.8 Help Menu

3.8.1 Tell Teledyne LeCroy

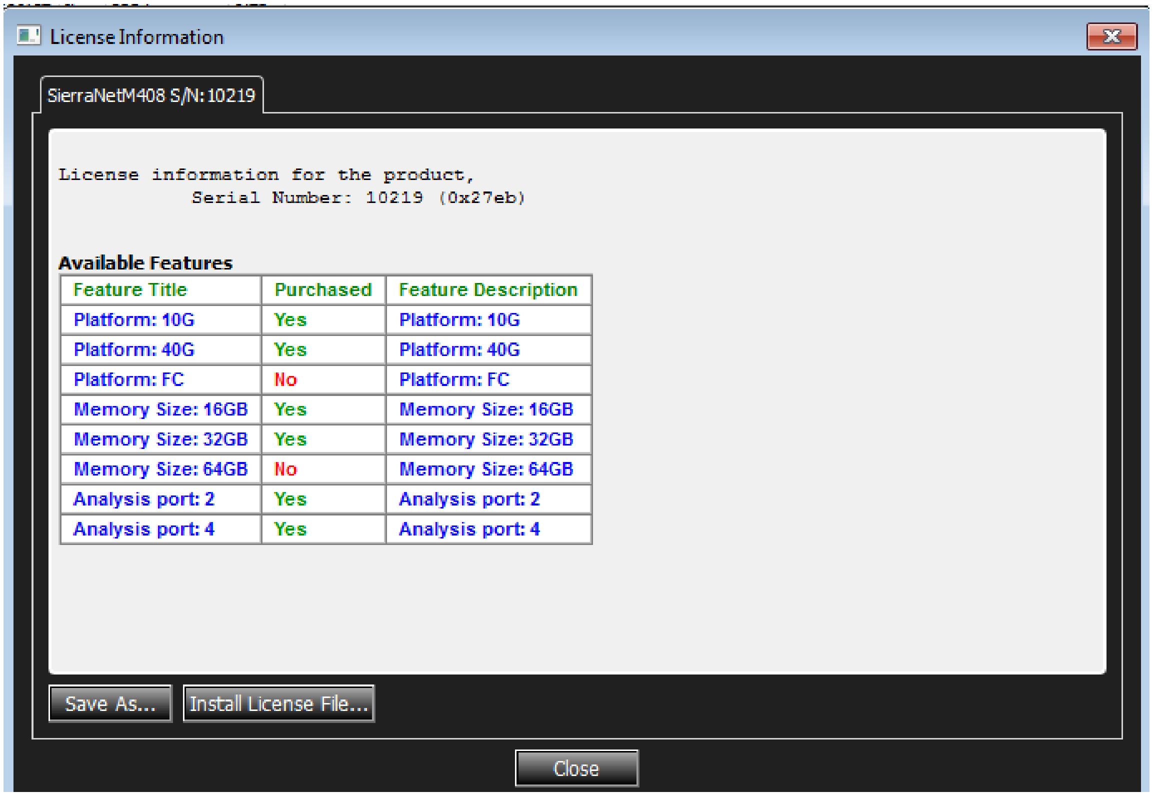
Report a problem to Teledyne LeCroy Support via e-mail by selecting **Help>Tell Teledyne LeCroy** from the application toolbar. This requires that an e-mail client be installed and configured on the host machine.

3.8.2 Help Topics

Displays online help. You can also select F1.

3.8.3 License Information

Open the license information dialog (see Figure 3.58 on page 161) to display a list of named features supported by the current software version. Named features that are not enabled on your system are indicated by No in the Purchased column. Whether or not named features are enabled depends on the license key stored in your analyzer. If you try to use a feature for which you do not yet have a license, the program displays the License Protection Message. To use the feature, you must purchase a license.



```
License information for the product,
          Serial Number: 10219 (0x27eb)
```

Available Features

Feature Title	Purchased	Feature Description
Platform: 10G	Yes	Platform: 10G
Platform: 40G	Yes	Platform: 40G
Platform: FC	No	Platform: FC
Memory Size: 16GB	Yes	Memory Size: 16GB
Memory Size: 32GB	Yes	Memory Size: 32GB
Memory Size: 64GB	No	Memory Size: 64GB
Analysis port: 2	Yes	Analysis port: 2
Analysis port: 4	Yes	Analysis port: 4

Figure 3.58: License Information Dialog

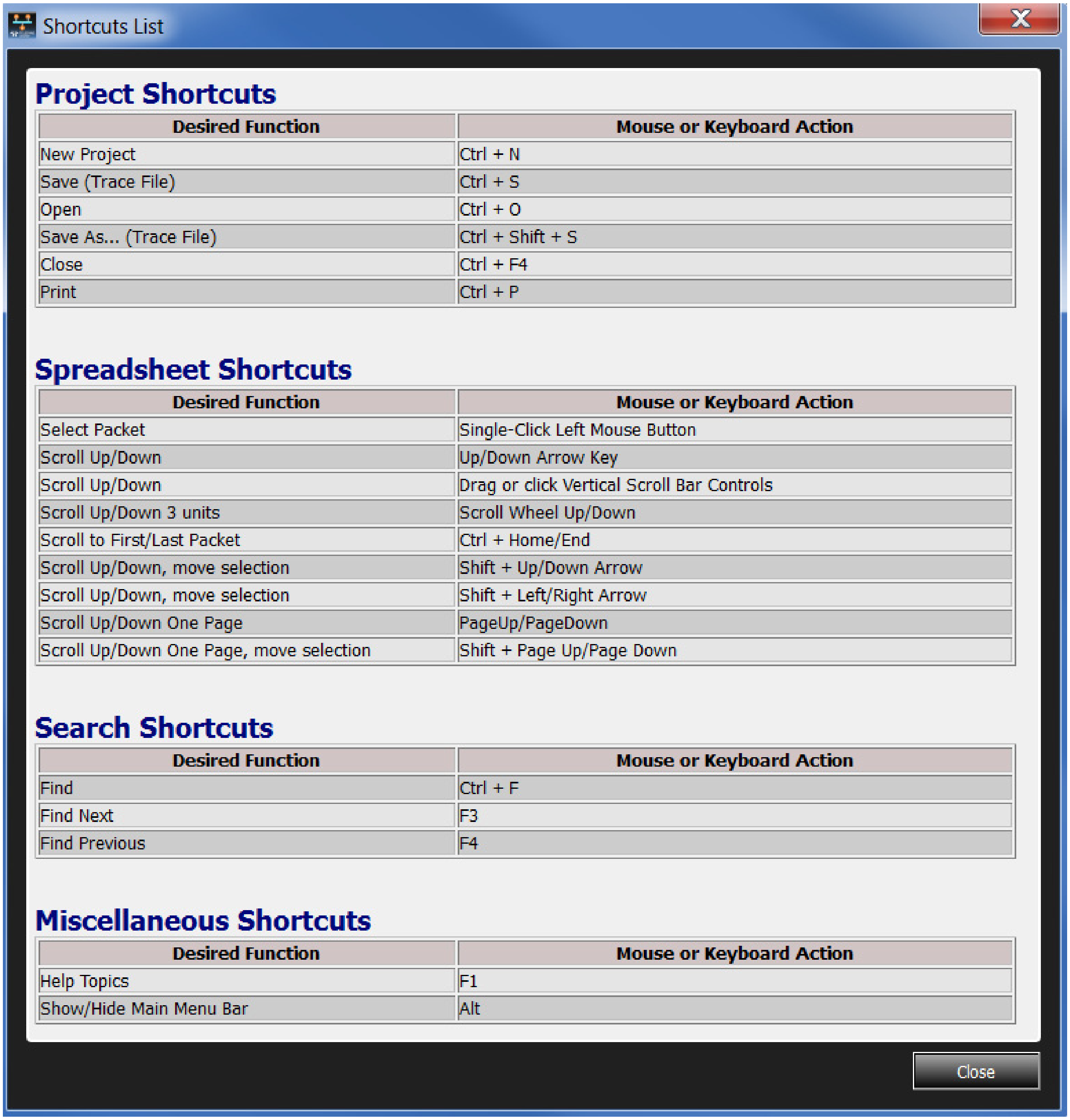
A current license agreement with Teledyne LeCroy entitles the Analyzer owner to continued technical support and access to software updates as they are published on the Teledyne LeCroy website. When you obtain a license key, from the Help menu in the License Information dialog, select **Install License File** to display the Open License dialog. Enter the path and filename for the license key, or browse to the directory that contains the license key and select the *.lic file. Click Open.

3.8.4 Check for Updates

Check whether a new software version is available. If so, you can download from the Teledyne LeCroy web site.
You can select to Check for updates at application startup.

3.8.5 Shortcut List

Displays a list of keyboard shortcuts.



Project Shortcuts

Desired Function	Mouse or Keyboard Action
New Project	Ctrl + N
Save (Trace File)	Ctrl + S
Open	Ctrl + O
Save As... (Trace File)	Ctrl + Shift + S
Close	Ctrl + F4
Print	Ctrl + P

Spreadsheet Shortcuts

Desired Function	Mouse or Keyboard Action
Select Packet	Single-Click Left Mouse Button
Scroll Up/Down	Up/Down Arrow Key
Scroll Up/Down	Drag or click Vertical Scroll Bar Controls
Scroll Up/Down 3 units	Scroll Wheel Up/Down
Scroll to First/Last Packet	Ctrl + Home/End
Scroll Up/Down, move selection	Shift + Up/Down Arrow
Scroll Up/Down, move selection	Shift + Left/Right Arrow
Scroll Up/Down One Page	PageUp/PageDown
Scroll Up/Down One Page, move selection	Shift + Page Up/Page Down

Search Shortcuts

Desired Function	Mouse or Keyboard Action
Find	Ctrl + F
Find Next	F3
Find Previous	F4

Miscellaneous Shortcuts

Desired Function	Mouse or Keyboard Action
Help Topics	F1
Show/Hide Main Menu Bar	Alt

Figure 3.59: Shortcuts List

3.8.6 About

Displays Teledyne LeCroy SierraNet Protocol Suite software version information.

Chapter 4

InFusion

4.1 InFusion Overview

The Teledyne LeCroy InFusion™ Error Injector and Traffic Modifier is an error injector and traffic modification tool that allows you to verify real-world fault handling for Fibre Channel systems. InFusion can sit unobtrusively in the data path on a live system to programmatically alter or corrupt traffic. InFusion is the ideal tool for stress-testing systems using actual workloads. Click the New Scenario icon to display the Infusion Scenario Manager dialog.

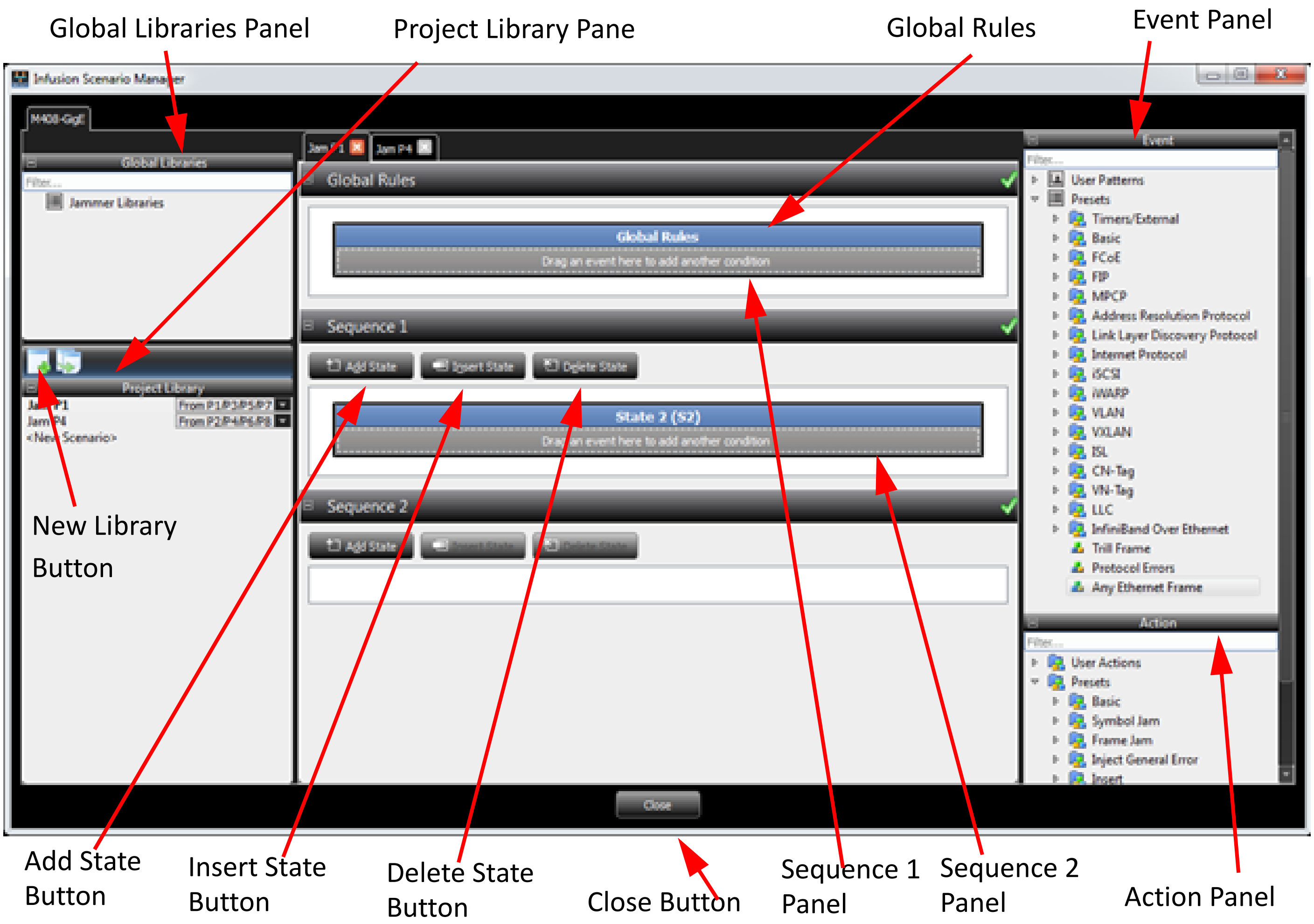


Figure 4.1: InFusion Windows

InFusion supports Ethernet and Fibre Channel links up to 16 Gbps. InFusion monitors traffic from both directions in real-time and relies on predefined rules to replace any bit, ordered-set, or parameter with one you specify. InFusion can change traffic when it detects a specific sequence or reaches a designated time interval, yet it requires no complicated scripts, programming, or simulation tools. It supports “Jumbo” packets up to 16K.

InFusion can monitor traffic in both directions and act on Events occurring in either direction of the communications link. InFusion can modify traffic in only one direction within a given test Scenario, but that direction can be either from the Originator or from the Responder.

InFusion is specifically designed to verify recovery characteristics within a subsystem. An easy, user friendly menu interface with icons and hyperlinks allows you to create specific test Scenarios in just minutes.

Once an InFusion session starts, the system automatically handles protocol handshaking between devices. InFusion transmits a faithful copy of the original data stream down to the CRC value which, if needed, it recalculates. InFusion allows test engineers to systematically verify error recovery in ways not possible with other test platforms.

4.2 Key Features

The key features of InFusion are:

- **Error Injection**: Injects CRC, disparity, 8b/10b encoding, framing, and coding errors.
- **Break Link Recovery**: Programmatically breaks the connection to test link recovery.
- **Value Replacement**: Monitors the link for specific values, patterns, or ordered-sets (as low as bit level) and replace with user-defined values. You can replace values on every occurrence, after a specified number of occurrences, or after a specified time interval.
- **Packet Drop**: Removes individual ordered-sets or frames from the stream to verify retry behavior.
- **Ordered-set Manipulation**: Replaces handshaking and flow control ordered-sets to help validate robustness of a design.
- **Traffic Monitoring:** Operates as a traffic monitor, collecting statistical data on user-specified parameters. In this mode, data passes unchanged in both directions.
- **Menu-Driven Interface:** Allows easy set-up of test Scenarios.

With respect to traffic modification, in the Link Layer you can modify ordered-sets, CRC, scrambled data, and connection Events. You cannot modify clock skew management and signal integrity.

InFusion consists of a hardware device that connects to the line under test and a Windows-based software application used to create and download test scripts to the device. You also can use the software application to configure and control the device across an Ethernet or USB link.

InFusion test scripts are called Scenarios. Scenarios determine how the hardware device monitors and modifies line traffic. In order to create and download Scenarios the Teledyne LeCroy Net Protocol Suite application must be used.

For the InFusion connections, the device is connected between the PHYs of the originator and responder.

4.3 Infusion Control Interface

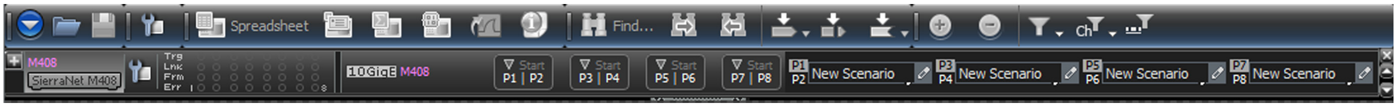


Figure 4.2: InFusion Control Interface Menu

The InFusion Control interface has the following controls:

Start/Stop Session button: This is a toggle button that starts or stops the session on the specified ports. Each port-pair has its own button and is controlled independently. The text on the bottom half of the button indicates the port-pair controlled by the button.

Scenario drop-down list: This is a drop-down list that lets you assign a scenario from the Project’s library to the specified ports. Each port-pair has its own drop-down list and is assigned independently. The text on the left side of the drop-down list indicates the port-pair to which the scenario is assigned. The highlighted port label indicates the direction of jamming, which can be changed from the Scenario Manager interface (see section “Traffic Direction” on page 199).

4.4 InFusion Scenario Manager Interface

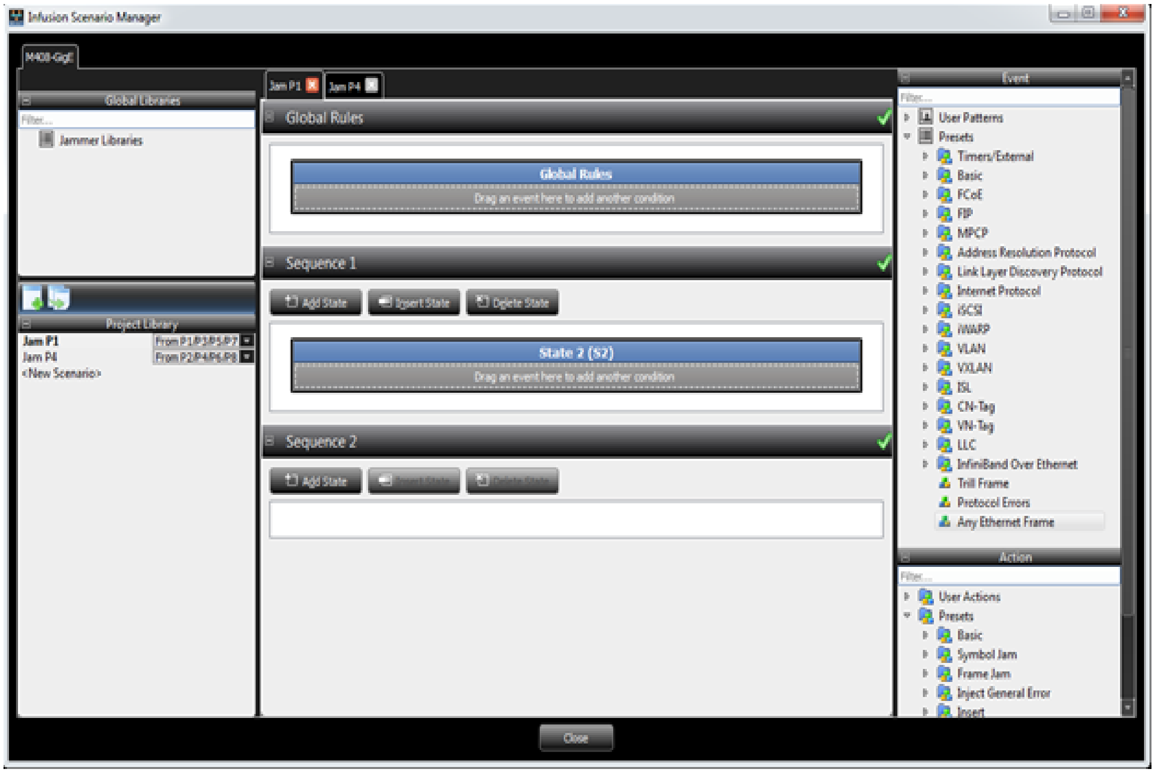


Figure 4.3: InFusion Scenario Manager Menu

The InFusion Scenario Editor interface has the following panels:

Global Libraries Panel: The Main Library window (on the left), which displays the available Scenarios. You can create a New Scenario, Open Containing Folder, Copy Container Folder Path, Add New Library, Rename Library or Remove Library. The scenarios saved on a specific platform in the Global Library are available in all projects for the same platform.

Project Library Panel: The Project Library window (on the left), which displays the project libraries. The scenarios saved in the Project Library are only available for the current project.

Scenarios Workspace Panel: This is the middle section, where you will construct and manipulate the logic of the scenario by defining Events and Actions.

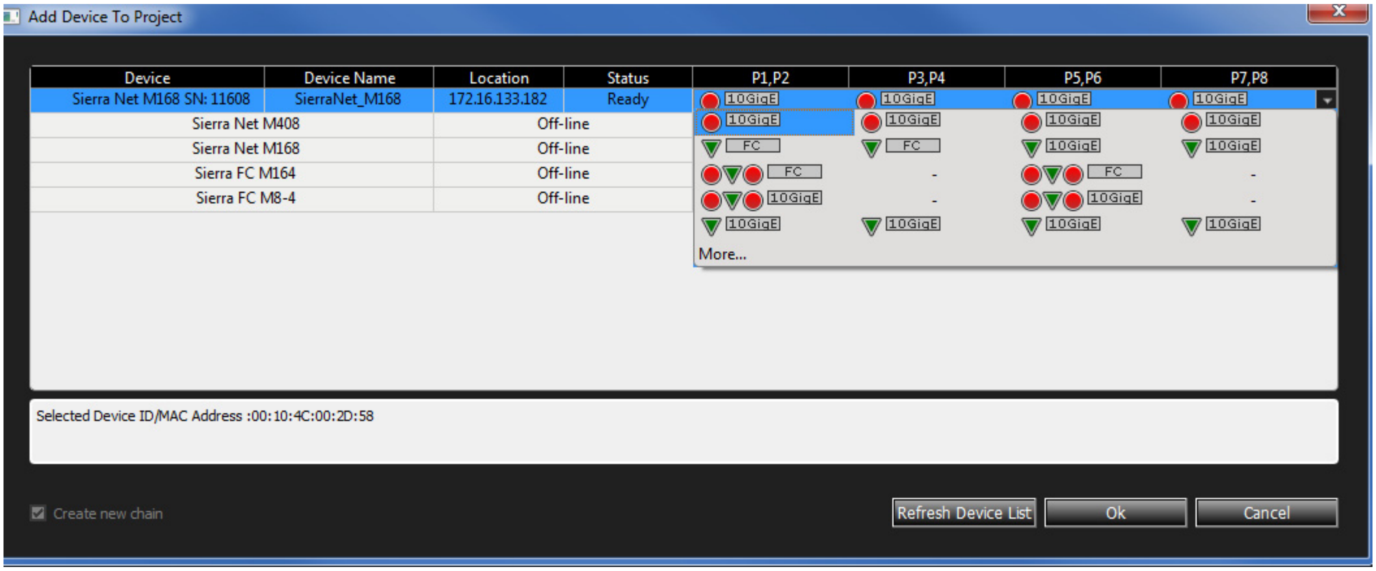
Event Panel: Lists all the available events to be used in the Scenarios Workspace.

Action Panel: Lists all the available actions to be used in the Scenarios Workspace.

4.5 Port Configuration for InFusion

Select **File> New Project** to display the Add Device to Project dialog (see (Figure 4.4 on page 167).

To record traffic both before and after the InFusion modifies (jams) it, select **AJA** (**Analyzer/Jammer/Analyzer**) in the Link Assignment column **(**or any other desired configuration) and click **OK**.



Add Device To Project

Device	Device Name	Location	Status	P1,P2	P3,P4	P5,P6	P7,P8
Sierra Net M168 SN: 11608	SierraNet_M168	172.16.133.182	Ready	● 10GigE	● 10GigE	● 10GigE	● 10GigE
Sierra Net M408		Off-line					
Sierra Net M168		Off-line					
Sierra FC M164		Off-line					
Sierra FC M8-4		Off-line					

● 10GigE	● 10GigE	● 10GigE	● 10GigE
▼ FC	▼ FC	▼ 10GigE	▼ 10GigE
●▼● FC	-	●▼● FC	-
●▼● 10GigE	-	●▼● 10GigE	-
▼ 10GigE	▼ 10GigE	▼ 10GigE	▼ 10GigE
More...			

Selected Device ID/MAC Address :00:10:4C:00:2D:58

Figure 4.4: Add Device to Project Dialog

Note: You can select only one Jammer port at a time when using the AJA configuration.

To record traffic from other ports after the InFusion modifies (jams) them, select a combination of ports that have **Jammer/Analyzer** specified under them. The different configurations accommodate different possible user setups and requirements.

Important Information for Jammer and Analyzer

Jammer intercepts and delays traffic on both directions simultaneously, so Originator sends to Jammer, Jammer delays and sends to Responder, Responder sends to Jammer, Jammer delays and sends to Originator. However, Jammer modifies traffic in one direction only: from Originator to Responder, or from Responder to Originator.

When AJAJ is selected, use a jumper between P2 and P3. For Bi directional jams, use P1/2 Jammer for "A" channel ("before" should be on 1 and "after" should be on 3) and use P3/4 Jammer for "B" channel ("before" should be on 4 and "after" should be on 2).

4.6 InFusion Scenarios

You can create and execute InFusion Scenarios. A Scenario is a test script that defines how InFusion monitors and modifies line traffic.

4.6.1 Scenario Overview

You create Scenarios on a host machine running the Net Protocol Suite application. You then specify the Scenarios for execution on an InFusion device.

The Net protocol Suite application provides a user friendly interface for building Scenarios. The interface prompts you for simple decisions and choices from drop-down menus and icons and has a drag and drop interface. As you make your selections, the script takes shape automatically in the Scenario window.

You can open an existing Library or create a new Library from the drop-down list on the top of the screen or click the New Scenario ✎ icon to display the Infusion Scenario Manager dialog.

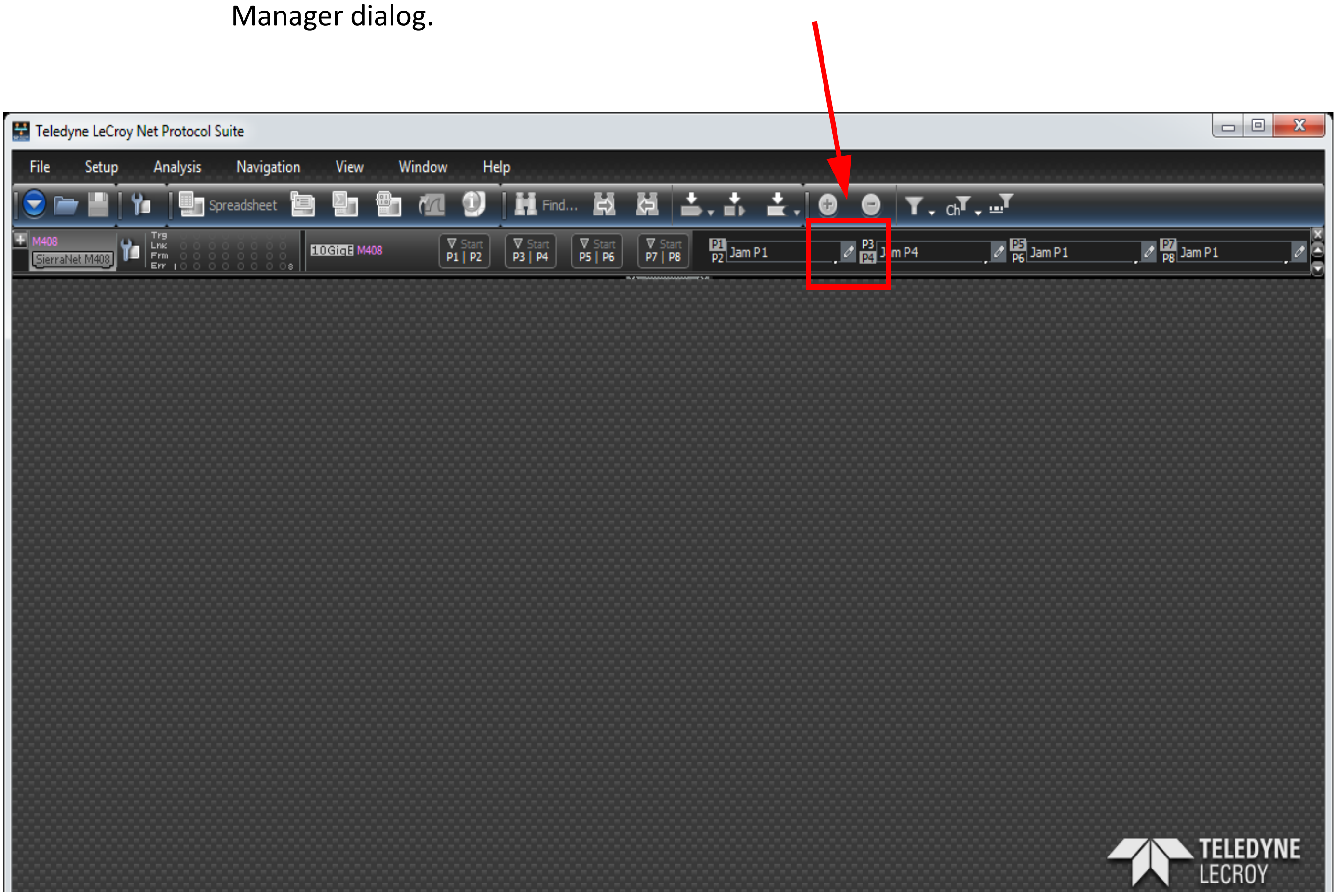
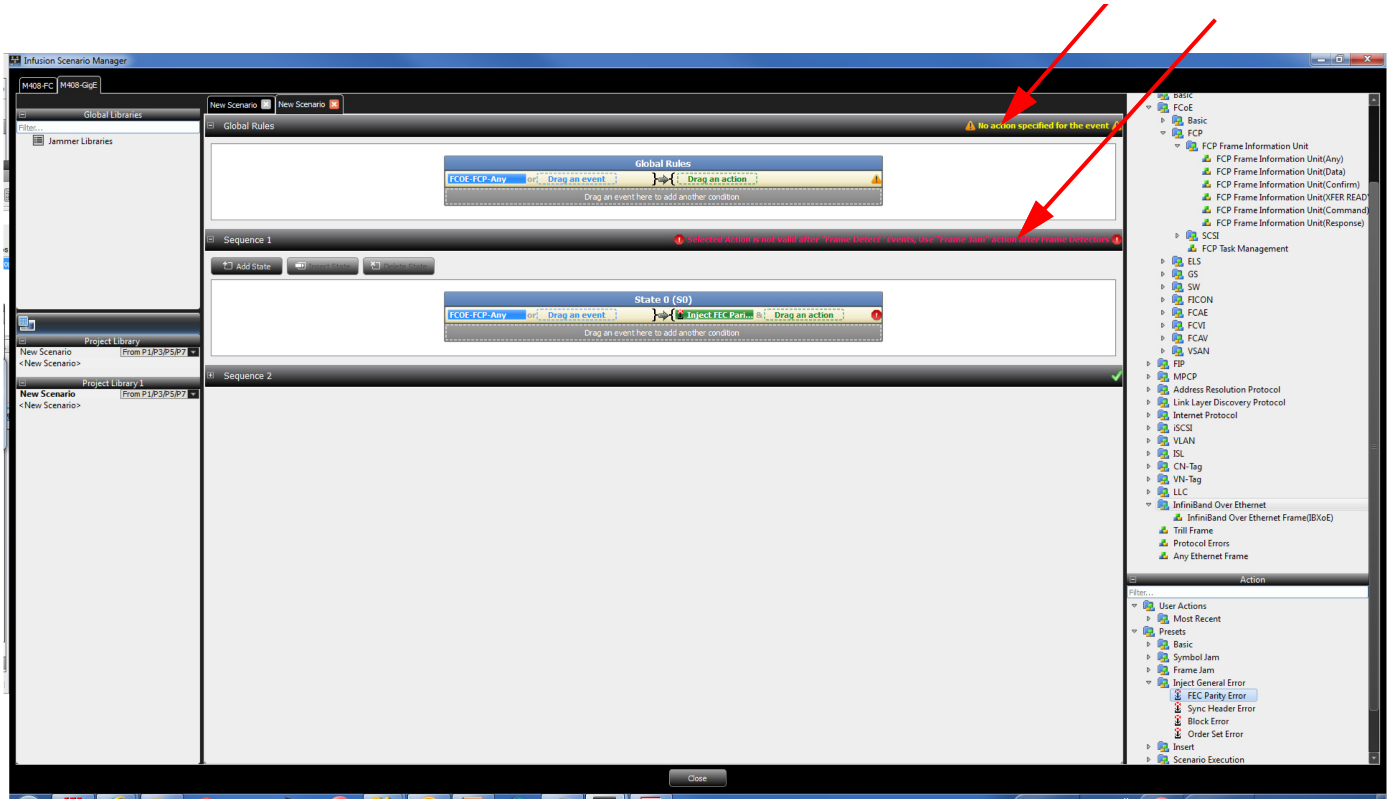


Figure 4.5: New Scenario in InFusion Scenario Manager.

You can drag and drop events in the Global Rules panel and assign actions to them.

Click the **Add State** button to drag and drop events in the Sequence 1 and Sequence 2 panels and assign actions to them. If Actions are not assigned a yellow Caution message displays. If invalid actions are assigned then a red Warning icon displays.



⚠ No action specified for the event ⚠

❗ Selected Action is not valid after "Frame Detect" Events, Use "Frame Jam" action after Frame Detectors ❗

Figure 4.6: Add State InFusion Scenario Manager

Note: The **Insert State** command inserts a new state after the current state. Plan carefully while creating scenarios or you might have to insert a state after state 0, copy and paste from state 0 to the new state, and clear out state 0, in order to accomplish what "Insert State" does.

The Global Rules and States are part of the new Scenario. Once the scenario is created, right-click on the New Scenario tab and select **Rename** to name it in the Project Library panel. Click the **Close** icon to save it in the Library for later use. All the Scenarios that are created are displayed in the Library panel.

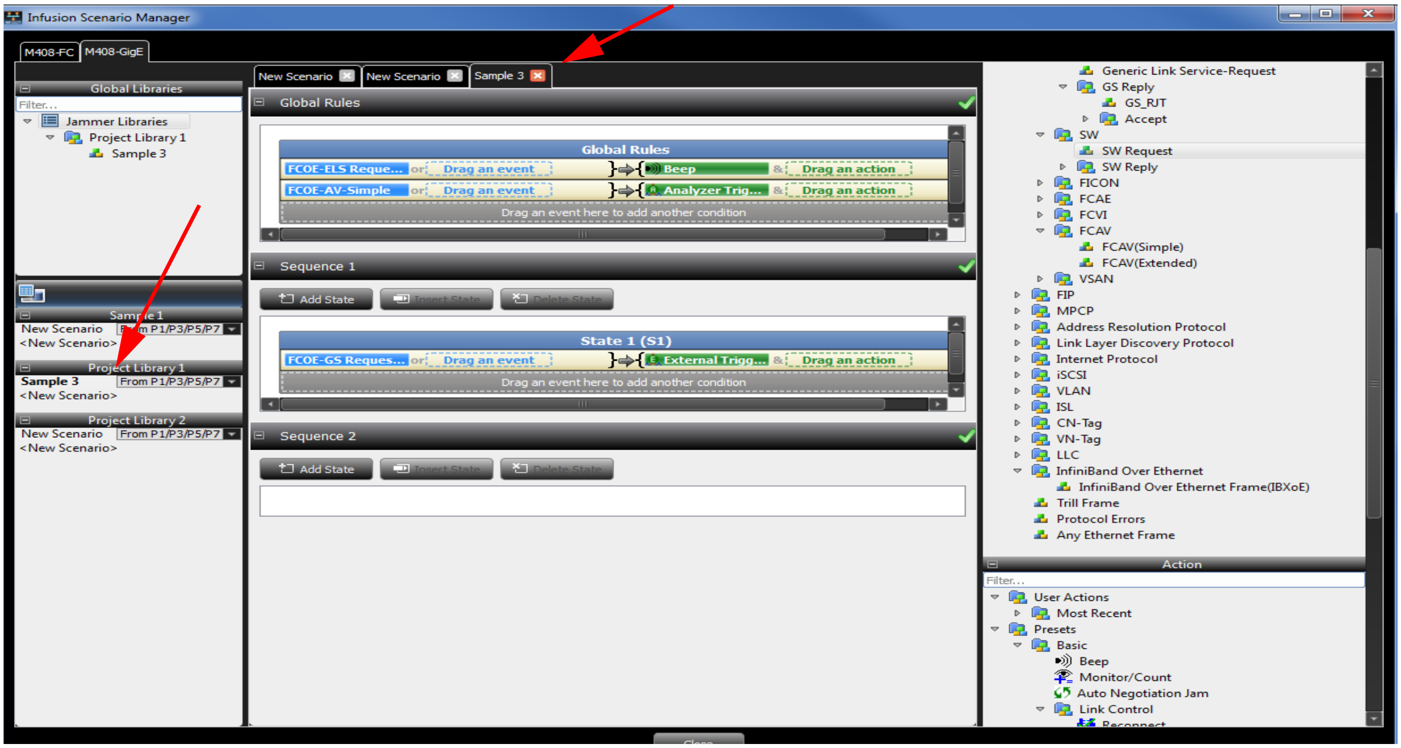


Figure 4.7: Global Rules and States InFusion Scenario Manager

4.6.2 Jam Details

- Jam Event: Set a Jam Event by dragging an Event to the Global Rules or Sequence panel. The Events and their descriptions are listed in Table 4.1 on page 171.
- Jam Action: Set a Jam Action by dragging an Action to the Global Rules or Sequence panel.
- After the first Jam Action has been specified you can set a consequent Jam Action by dragging more Actions to the **Drag an Event here to add another condition** area. The Jam Actions and their descriptions are listed in Table 4.1 on page 171.

4.6.3 Scenario Events

Table Table 4.1 on page 171 describes the Presets that can be used as FCoE Events. See “Available Resources” on page 191 for details.

Note: You can have multiple Events and Actions in Global Rules and in each State.

TABLE 4.1: Events and their Descriptions (Ethernet)

Event	Description
User Patterns	
Most Recent	Lists the most recent Events.
New User Group	Lists the new user groups.
Presets	
Timers/External	
Timer	The Event occurs when the timer expires.
Other Trigs	Analyzer: the Event occurs when the Analyzer triggers. External: the Event occurs when the external Trigger In is asserted.
Basic	
Basic Link Service	Refer to section "Basic" on page 77.
Link Control Frame	Refer to section "Link Control Frame" on page 78.
Link Speed	The Event occurs when the link is at the specified speed.
Both Linkup	The Event occurs when both ports are out of electric idle.
Dword Reuse	Refer to section "Using Captured Data Dwords" on page 193.
Dword Matcher	Refer to section "Dword Matcher" on page 195.
Training Sequence	**Inject Error on Control**: Generates Manchester Coding violation on Control field bits corresponding to the defined mask: One means violation, and zero means no error. **Inject Error on Status**: Generates Manchester Coding violation on Status field bits corresponding to the defined mask: One means violation, and zero means no error. **Frame Marker Error**: Generates training sequence with an invalid frame marker. **Recode Manchester Coding**: Forces jammer to recalculate Manchester Coding for each bit of training frame.
FCP	
FCP SCSI Command	Refer to section "Basic" on page 77.
FCP Frame Information Unit	Refer to section "FCP Patterns" on page 79.
SCSI Command Status	Refer to section "SCSI" on page 79.
FCP Task Management	Refer to section "FCP Task Management" on page 80.
ELS	
Extended Link Service-Request	Refer to section "ELS Patterns" on page 80.
Extended Link Service-Request, Reply	Refer to section "ELS Patterns" on page 80.
Extended Link Service-Reply	Refer to section"ELS Patterns" on page 80.

Event	Description
GS	
Generic Link Service-Request	Refer to section "GS Patterns" on page 80.
Generic Link Service-Request, Reply	Refer to section "GS Patterns" on page 80.
Generic Link Service-Reply	Refer to section "GS Patterns" on page 80.
SW	
Switch Internal Link - Request	Refer to section "SW Patterns" on page 80.
Switch Internal Link - Request, Reply	Refer to section "SW Patterns" on page 80.
Switch Internal Link - Reply	Refer to section "SW Patterns" on page 80.
FICON	
FICON (Any Data Information Block Type)	Refer to section "FICON Patterns" on page 80.
FICON (Data)	Refer to section Refer to section "FICON Patterns" on page 80.
FICON (Command)	Refer to section Refer to section "FICON Patterns" on page 80
FICON (Status)	Refer to section Refer to section "FICON Patterns" on page 80.
FICON (Control)	Refer to section Refer to section "FICON Patterns" on page 80.
FICON (Command-Data)	Refer to section "FICON Patterns" on page 80.
FICON (Link-Control)	Refer to section "FICON Patterns" on page 80.
FCAE 1553	
FCAE - ASM	Refer to section "FCAE_ASM" on page 80.
FCAE 1553 (Any)	Refer to section "FCAE-1553" on page 80.
FCAE 1553 (Data)	Refer to section "FCAE-1553" on page 80.
FCAE 1553 (Command)	Refer to section "FCAE-1553" on page 80.
FCAE 1553 (Status)	Refer to section "FCAE-1553" on page 80.
FCVI	
FCVI(Any)	Refer to section "FCVI Patterns" on page 80.
FCVI(SEND_RQST)	Refer to section "FCVI Patterns" on page 80.
FCVI(WRITE_RQST)	Refer to section "FCVI Patterns" on page 80.
FCVI(READ_RQST)	Refer to section "FCVI Patterns" on page 80.
FCVI(SEND_RESP)	Refer to section "FCVI Patterns" on page 80.
FCVI(WRITE_RESP)	Refer to section "FCVI Patterns" on page 80.
FCVI(READ_RESP)	Refer to section "FCVI Patterns" on page 80.
FCVI(CONNECT_RQST)	Refer to section "FCVI Patterns" on page 80.

Event	Description
FCVI(DISCONNECT_RQST)	Refer to section "FCVI Patterns" on page 80.
FCVI(CONNECT_RESP1)	Refer to section "FCVI Patterns" on page 80.
FCVI(CONNECT_RESP2)	Refer to section "FCVI Patterns" on page 80.
FCVI(CONNECT_RESP3)	Refer to section "FCVI Patterns" on page 80.
FCVI (DISCONNECT_RESP)	Refer to section "FCVI Patterns" on page 80.
FCAV	
FCAV(Simple)	Refer to section "FCAV Patterns" on page 80.
FCAV(Extended)	Refer to section "FCAV Patterns" on page 80.
VSAN	
Basic	
VSAN-Basic Link Service	Refer to section "VSAN Patterns" on page 80.
VSAN-Link Control Frame	Refer to section "VSAN Patterns" on page 80.
FCP	
VSAN-FCP SCSI Command	Refer to section "VSAN Patterns" on page 80.
VSAN-FCP Frame Information Unit	Refer to section "VSAN Patterns" on page 80.
VSAN-SCSI Command Status	Refer to section "VSAN Patterns" on page 80.
VSAN-FCP Task Management	Refer to section "VSAN Patterns" on page 80.
ARB	
VSAN-ARB Loop Initialization	Refer to section "VSAN Patterns" on page 80.
ELS	
VSAN-Extended Link Service-Request	Refer to section "VSAN Patterns" on page 80.
VSAN-Extended Link Service-Reply	Refer to section "VSAN Patterns" on page 80.
GS	
VSAN-Generic Link Service-Request	Refer to section "VSAN Patterns" on page 80.
VSAN-Generic Link Service-Reply	Refer to section "VSAN Patterns" on page 80.
SW	
VSAN-Switch Internal Link-Request	Refer to section "VSAN Patterns" on page 80.
VSAN-Switch Internal Link-Reply	Refer to section "VSAN Patterns" on page 80.
FICON	

Event	Description
VSAN-FICON (Any Data Information Block Type)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Data)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Command)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Status)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Control)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Command-Data)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Link-Control)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCAE-ASM	Refer to section "VSAN Patterns" on page 80.
VSAN-FCAE 1553	
VSAN-FCAE 1553 (Any)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCAE 1553 (Data)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCAE 1553 (Command)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCAE 1553 (Status)	Refer to section "VSAN Patterns" on page 80.
FCVI	
VSAN-FCVI(Any)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(SEND_RQST)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(WRITE_RQST)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(READ_RQST)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(SEND_RESP)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(WRITE_RESP)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(READ_RESP)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(CONNECT_RQST)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(DISCONNECT_RQST)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(CONNECT_RESP1)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(CONNECT_RESP2)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(CONNECT_RESP3)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCVI(DISCONNECT_RESP)	Refer to section "VSAN Patterns" on page 80.
FCAV	
VSAN-FCAV(Simple)	Refer to section "VSAN Patterns" on page 80.
VSAN-FCAV(Extended)	Refer to section "VSAN Patterns" on page 80.

Event	Description
FIP	Refer to section “FIP Patterns” on page 81.
MPCP	Refer to section “MPCP Pattern” on page 82.
Address Resolution Protocol	Refer to section “Address Resolution Protocol Pattern” on page 82.
Link Layer Discovery Protocol	Refer to section “Link Layer Discovery Protocol Pattern” on page 83.
Internet Protocol	Refer to section “Internet Protocol Pattern” on page 84.
iSCSI	Refer to section “iSCSI Pattern” on page 84.
VLAN	Refer to section “VLAN Patterns” on page 87.
ISL	Refer to section “ISL Patterns” on page 87.
CN-Tag	Refer to section “CN Tag Patterns” on page 88.
VN-Tag	Refer to section “VN Tag Patterns” on page 88.
Trill Frame	Refer to section “LLC” on page 88.
Protocol Errors	Refer to section “Protocol Errors” on page 92.
Jammer Internal Triggers	Refer to section “Synch Jammer Scenarios with Jammer Internal Triggers” on page 206.

The following table describes the Presets that can be used as FC Events.

TABLE 4.2: Events and their Descriptions (FC)

Event	Description
User Patterns	
Most Recent	Lists the most recent Events.
New User Group	Lists the new user groups.
Presets	
Timers/External	
Timer	The Event occurs when the timer expires.
Other Trigs	Analyzer: the Event occurs when the Analyzer triggers. External: the Event occurs when the external Trigger In is asserted.
Basic	
Ordered Set	Refer to section "Ordered Set" on page 95.
Basic Link Service	Refer to section "Basic Link Service" on page 99.
Link Control Frame	Refer to section "Link Control Frame" on page 100.
Link Speed	The Event occurs when the link is at the specified speed.
Both Linkup	The Event occurs when both ports are out of electric idle.
Training Sequence	**Inject Error on Control**: Generates Manchester Coding violation on Control field bits corresponding to the defined mask: One means violation, and zero means no error. **Inject Error on Status**: Generates Manchester Coding violation on Status field bits corresponding to the defined mask: One means violation, and zero means no error. **Frame Marker Error**: Generates training sequence with an invalid frame marker. **Recode Manchester Coding**: Forces jammer to recalculate Manchester Coding for each bit of training frame. Refer to section "Training Sequence" on page 98.
FCP	
FCP SCSI Command	Refer to section "SCSI" on page 79.
FCP Frame Information Unit	Refer to section "Frame Information Unit" on page 79.
SCSI Command Status	Refer to section "SCSI" on page 79.
FCP Task Management	Refer to section "FCP Task Management" on page 80.
ELS	
Extended Link Service-Request	Refer to section "ELS Patterns" on page 80.
Extended Link Service-Request, Reply	Refer to section "ELS Patterns" on page 80.
Extended Link Service-Reply	Refer to section"ELS Patterns" on page 80.
GS	

Event	Description
Generic Link Service-Request	Refer to section "Generic Link Service-Request" on page 80.
Generic Link Service-Request, Reply	Refer to section "GS Reply" on page 80.
Generic Link Service-Reply	Refer to section "GS Reply" on page 80.
SW	
Switch Internal Link - Request	Refer to section "SW Request" on page 80.
Switch Internal Link - Request, Reply	Refer to section "SW Reply" on page 80.
Switch Internal Link - Reply	Refer to section "SW Reply" on page 80.
FICON	
FICON (Any Data Information Block Type)	Refer to section "FICON Patterns" on page 80.
FICON (Data)	Refer to section Refer to section "FICON Patterns" on page 80.
FICON (Command)	Refer to section Refer to section "FICON Patterns" on page 80.
FICON (Status)	Refer to section Refer to section "FICON Patterns" on page 80.
FICON (Control)	Refer to section Refer to section "FICON Patterns" on page 80.
FICON (Command-Data)	Refer to section "FICON Patterns" on page 80.
FICON (Link-Control)	Refer to section "FICON Patterns" on page 80.
FCAE 1553	
FCAE - ASM	Refer to section "FCAE_ASM" on page 80.
FCAE 1553 (Any)	Refer to section "FCAE-1553" on page 80.
FCAE 1553 (Data)	Refer to section "FCAE-1553" on page 80.
FCAE 1553 (Command)	Refer to section "FCAE-1553" on page 80.
FCAE 1553 (Status)	Refer to section "FCAE-1553" on page 80.
FCVI	
FCVI(Any)	Refer to section "FCVI Patterns" on page 80.
FCVI(SEND_RQST)	Refer to section "FCVI Patterns" on page 80.
FCVI(WRITE_RQST)	Refer to section "FCVI Patterns" on page 80.
FCVI(READ_RQST)	Refer to section "FCVI Patterns" on page 80.
FCVI(SEND_RESP)	Refer to section "FCVI Patterns" on page 80.
FCVI(WRITE_RESP)	Refer to section "FCVI Patterns" on page 80.
FCVI(READ_RESP)	Refer to section "FCVI Patterns" on page 80.
FCVI(CONNECT_RQST)	Refer to section "FCVI Patterns" on page 80.
FCVI(DISCONNECT_RQST)	Refer to section "FCVI Patterns" on page 80.

Event	Description
FCVI(CONNECT_RESP1)	Refer to section "FCVI Patterns" on page 80.
FCVI(CONNECT_RESP2)	Refer to section "FCVI Patterns" on page 80.
FCVI(CONNECT_RESP3)	Refer to section "FCVI Patterns" on page 80.
FCVI (DISCONNECT_RESP)	Refer to section "FCVI Patterns" on page 80.
FCAV	
FCAV(Simple)	Refer to section "FCAV Patterns" on page 80.
FCAV(Extended)	Refer to section "FCAV Patterns" on page 80.
VSAN	
FCP	
VSAN-FCP SCSI Command	Refer to section "VSAN Patterns" on page 80.
VSAN-FCP Frame Information Unit	Refer to section "VSAN Patterns" on page 80.
VSAN-SCSI Command Status	Refer to section "VSAN Patterns" on page 80.
VSAN-FCP Task Management	Refer to section "VSAN Patterns" on page 80.
ARB	
VSAN-ARB Loop Initialization	Refer to section "VSAN Patterns" on page 80.
ELS	
VSAN-Extended Link Service-Request	Refer to section "VSAN Patterns" on page 80.
VSAN-Extended Link Service-Reply	Refer to section "VSAN Patterns" on page 80.
GS	
VSAN-Generic Link Service-Request	Refer to section "VSAN Patterns" on page 80.
VSAN-Generic Link Service-Reply	Refer to section "VSAN Patterns" on page 80.
SW	
VSAN-Switch Internal Link-Request	Refer to section "VSAN Patterns" on page 80.
VSAN-Switch Internal Link-Reply	Refer to section "VSAN Patterns" on page 80.
FICON	
VSAN-FICON (Any Data Information Block Type)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Data)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Command)	Refer to section "VSAN Patterns" on page 80.
VSAN-FICON (Status)	Refer to section "VSAN Patterns" on page 80.

Event	Description
VSAN-FICON (Control)	Refer to section “VSAN Patterns” on page 80.
VSAN-FICON (Command-Data)	Refer to section “VSAN Patterns” on page 80.
VSAN-FICON (Link-Control)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCAE-ASM	Refer to section “VSAN Patterns” on page 80.
VSAN-FCAE 1553	
VSAN-FCAE 1553 (Any)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCAE 1553 (Data)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCAE 1553 (Command)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCAE 1553 (Status)	Refer to section “VSAN Patterns” on page 80.
FCVI	
VSAN-FCVI(Any)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(SEND_RQST)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(WRITE_RQST)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(READ_RQST)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(SEND_RESP)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(WRITE_RESP)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(READ_RESP)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(CONNECT_RQST)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(DISCONNECT_RQST)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(CONNECT_RESP1)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(CONNECT_RESP2)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(CONNECT_RESP3)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCVI(DISCONNECT_RESP)	Refer to section “VSAN Patterns” on page 80.
FCAV	
VSAN-FCAV(Simple)	Refer to section “VSAN Patterns” on page 80.
VSAN-FCAV(Extended)	Refer to section “VSAN Patterns” on page 80.
FIP	Refer to section “FIP Patterns” on page 81.
MPCP	Refer to section “MPCP Pattern” on page 82.
Address Resolution Protocol	Refer to section “Address Resolution Protocol Pattern” on page 82.

Event	Description
Link Layer Discovery Protocol	Refer to section “Link Layer Discovery Protocol Pattern” on page 83.
Internet Protocol	Refer to section “Internet Protocol Pattern” on page 84.
iSCSI	Refer to section “iSCSI Pattern” on page 84 and “ISCSI Cmd” on page 86.
VLAN	Refer to section “VLAN Patterns” on page 87.
ISL	Refer to section “ISL Patterns” on page 87.
CN-Tag	Refer to section “CN Tag Patterns” on page 88.
VN-Tag	Refer to section “VN Tag Patterns” on page 88.
Trill Frame	Refer to section “Trill Frame” on page 90.
Protocol Errors	Refer to section “Protocol Errors” on page 92.
Jammer Internal Triggers	Refer to section “Synch Jammer Scenarios with Jammer Internal Triggers” on page 206.

Note: You can specify additional Sequences and States. The application automatically checks for the maximum number of terms (sequences/states). When you exceed the limit, an error is flagged, prompting you to jump to the place that caused the error.

Note: You can specify additional Sequences and States. The application automatically checks for the maximum number of terms (sequences/states). When you exceed the limit, an error is flagged, prompting you to jump to the place that caused the error.

Creating InFusion Scenarios is easy, but it requires an understanding of the following terms defined in Table 4.3.

TABLE 4.3: Key Scenario Terms

Term	Definition
Action	InFusion response to an Event. See “Scenario Actions” on page 181.
Event	Condition that is detectable by InFusion. See “Scenario Events” on page 170.
Combined Event	Logical OR association of Events (for example, Event A OR Event B).
Global Rules	Portion of a Scenario that can define a single InFusion test state. You can think of the Global Rules and each Sequence as a separate test routine or program operating within the Scenario. Each operates independently and in parallel with the others. The purpose of each is to detect Events and then respond with the appropriate Action or set of Actions. In essence, you can operate up to three test states simultaneously within InFusion - one is the Global Rules, and the other two are the 2 active states, one in each Sequence. See “Global Rules” on page 197.
Sequence	Portion of a Scenario that can define multiple InFusion test states. More flexible than the Global Rules, a Sequence allows more powerful Scenarios that include branching and looping between test states (Global Rules can define only a single test state, so there is no branching). See “Sequences” on page 198.
State	“Behavior” of the Global Rules or a Sequence at any point in time. In terms of InFusion testing, behavior is “waiting” for a set of Events and responding with a set of Actions.

4.6.4 Scenario Actions

After you enter the set of Events for a test state, the menu-driven interface prompts you for the corresponding Action or set of Actions. If you define multiple Actions, the Actions occur simultaneously.

Note: The Actions displayed are dependent on the Events selected.

The following figure displays the options for a set of Actions in the Simple Mode (Ethernet).

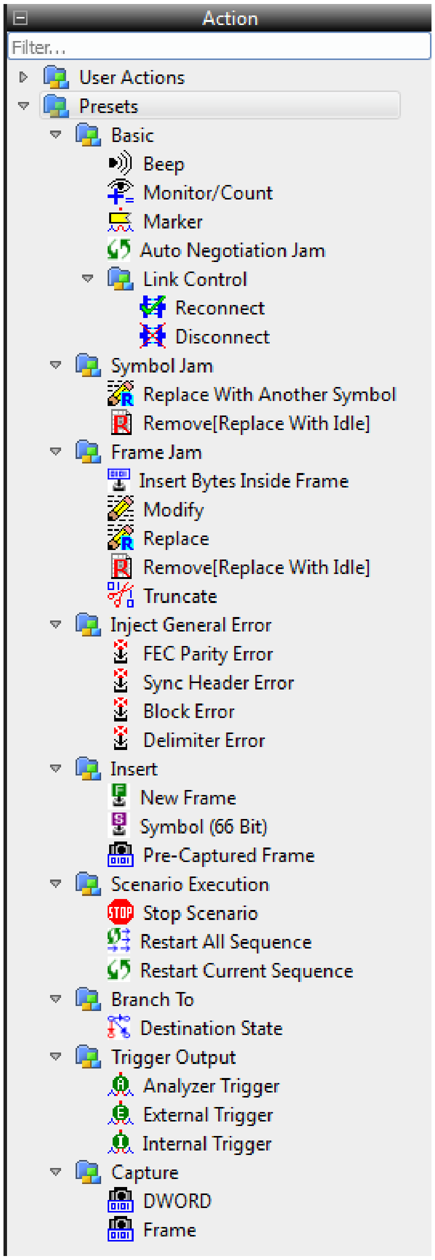


Figure 4.8: Ethernet Action Properties Dialog

The following table lists the supported Actions. Note that some of these Actions only apply to creating sequences.

TABLE 4.4: Test State Actions in Simple Mode

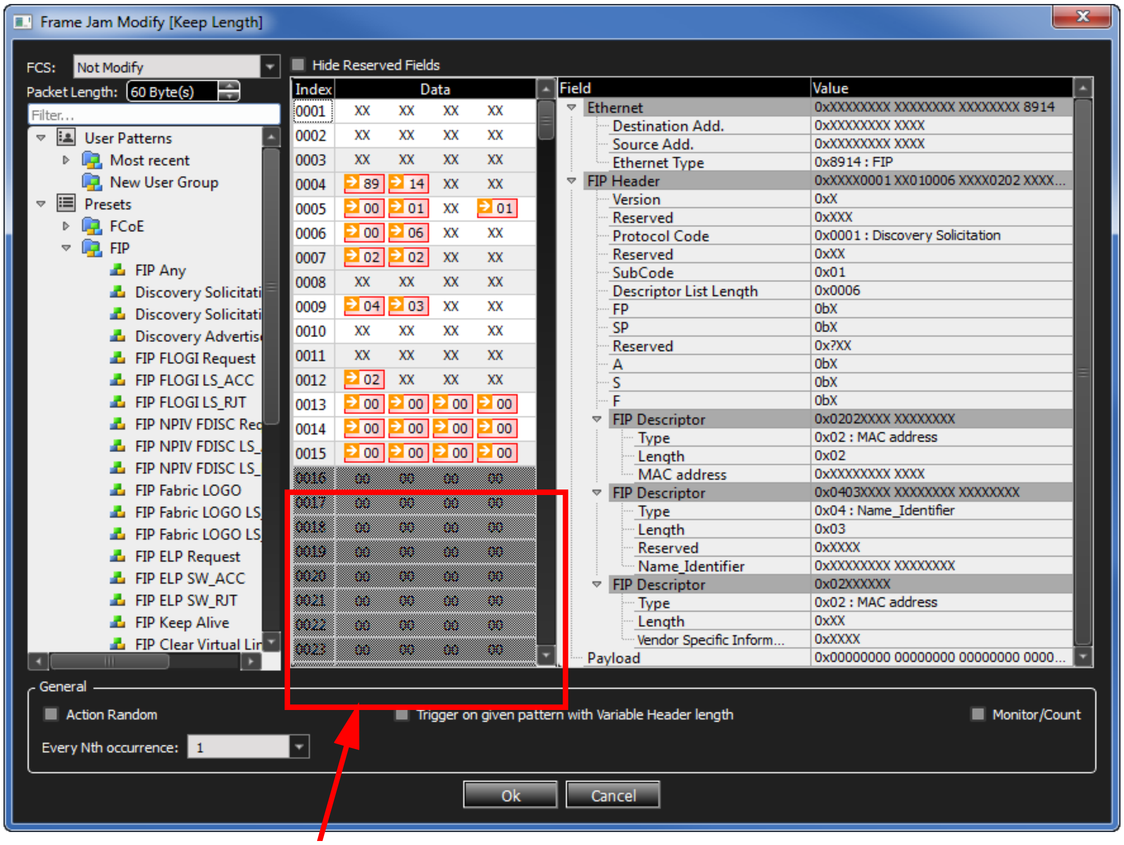
Action		Description
Basic	Beep	Emits audible sound of duration selectable via a drop-down list.
	Monitor Count –	Opens a window to count the number of Events that occur during a session. A session is a time interval during which a Scenario runs.
	Auto Negotiation Jam	Opens a window to set Code Values, Code Settings and General parameters (Ethernet only).
	Link Control	Reconnect - starts traffic pass-through immediately. This Action restarts traffic after a previous disconnect command. Once traffic is passing through, the originator and responder resume link bring up. Disconnect - puts InFusion ports at electrical idle immediately. This action is only in effect while the scenario is running, and the Jammer will reconnect the line when the scenario is stopped.
		Reconnect/Disconnect can be applied in either direction separately: From P1/P3/P5/P7 direction: Reconnect/ Disconnect only the originator link. From P2/P4/P6/P8 direction: Reconnect/ Disconnect only the responder link. (See Figure 4.11 on page 188.)
Symbol Jam	Replace with Another Symbol	Replaces the Symbol with the selected Symbol.
	Remove [Replace with Idle]	Removes the Symbol.
DWORD Jam	Replace DWORD	Replace DWORD (FC 16 only).

Action		Description
Frame Jam	Insert Bytes Inside Frame	Allows to insert up to 60 Bytes inside the frame, at the specified offset or at the “current” dword, meaning the dword that caused the Event.
	Modify [Keep Length]	Allows to manipulate each dword in the header, with the selected Action (click on Pass though to get a drop-down list).
	Replace	Replaces the whole frame with the selected frame.
	Remove [Replace with IDLE]	Removes the whole frame.
	Truncate	Removes some of the payload, as specified in the Frame Length.
Inject General Error	Invalid 10-bit-Error Code	Injects invalid 10b code into the line (FC8 only).
	Running Disparity Error	Injects a Running Disparity (RD) error into traffic(FC8 only).
	FEC Parity Error	Injects a FEC error into traffic.
	Sync Header Error	Injects a Sync Header error into traffic.
	Block Error	Injects a Block error into traffic.
	Order Set Error	Injects a Order Set error into traffic, (Not available with 40GigE).
Insert	Insert New Frame	Allows to insert a whole frame as specified from the list of available frames.
	Symbol (66 Bit)	Allows to insert a Symbol 66 bits.
	Pre-captured Frame	Allows to insert a Pre-captured Frame (Ethernet only).
	Insert Bytes	Allows to insert Bytes (FC 16 only).
Ordered Set Jam	Delete	Delete an Ordered Set Jam.
	Remove [Replace with IDLE]	Remove an Ordered Set Jam or Replace with another Ordered Set.
	Replace with Another Ordered Set	Only replace with another Ordered Set.
Scenario Execution	Stop Scenario	Stops the current Scenario. This Action should be the only Action in a State as it has higher priority over other Actions.
	Restart All Sequence	Restart all sequences in the Scenario.[1]
	Restart Current Sequence	Restart the sequence that contains this Action definition. [1]
Branch To	Destination State	Go to a state in this Sequence.[1]

Action		Description
Trigger Output		Sends a signal out the trigger port to the device downstream.
	Analyzer Trigger	1. The Action is to send a trigger to the Analyzer. 2. The trigger point in the Analyzer that caused the analyzer trigger action will not be the selected event, it will be the selected event with some offset.
	External Trigger Output	The Action is to cause an external trigger output.
	Marker Trigger	Add a marker to captured data.
Capture	DWORD	Capture DWORD.
		Reuse of Captured DWORDs. (See “Reusing “Captured DWORDS” in Events” on page 195.)
	Frame	Capture Frame (Ethernet only).

[1] Only shown in Action Properties dialog box when creating a sequence.

Changes made in the grey area in the screen below when modifying packets do not take effect and will not be jammed.



FCS: Not Modify

Packet Length: 60 Byte(s)

☐ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	89	14	XX	XX
0005	00	01	XX	01
0006	00	06	XX	XX
0007	02	02	XX	XX
0008	XX	XX	XX	XX
0009	04	03	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	02	XX	XX	XX
0013	00	00	00	00
0014	00	00	00	00
0015	00	00	00	00
0016	00	00	00	00
0017	00	00	00	00
0018	00	00	00	00
0019	00	00	00	00
0020	00	00	00	00
0021	00	00	00	00
0022	00	00	00	00
0023	00	00	00	00

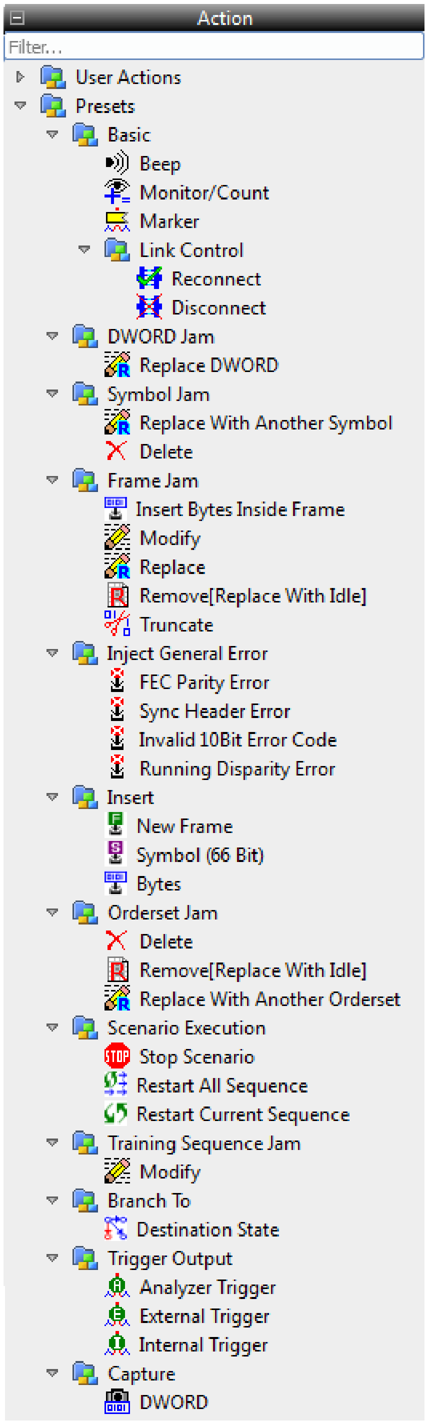
Field	Value
Ethernet	0xXXXXXXXX XXXXXXXX XXXXXXXX 8914
Destination Add.	0xXXXXXXXX XXXX
Source Add.	0xXXXXXXXX XXXX
Ethernet Type	0x8914 : FIP
FIP Header	0xXXXX0001 XX010006 XXXX0202 XXXX...
Version	0xX
Reserved	0xXXX
Protocol Code	0x0001 : Discovery Solicitation
Reserved	0xXX
SubCode	0x01
Descriptor List Length	0x0006
FP	0bX
SP	0bX
Reserved	0x?XX
A	0bX
S	0bX
F	0bX
FIP Descriptor	0x0202XXXX XXXXXXXX
Type	0x02 : MAC address
Length	0x02
MAC address	0xXXXXXXXX XXXX
FIP Descriptor	0x0403XXXX XXXXXXXX XXXXXXXX
Type	0x04 : Name_Identifier
Length	0x03
Reserved	0xXXXX
Name_Identifier	0xXXXXXXXX XXXXXXXX
FIP Descriptor	0x02XXXXXX
Type	0x02 : MAC address
Length	0xXX
Vendor Specific Inform...	0xXXXX
Payload	0x00000000 00000000 00000000 0000...

☐ Action Random ☐ Trigger on given pattern with Variable Header length ☐ Monitor/Count

Every Nth occurrence: 1

Figure 4.9: Frame Jam - Modify Dialog

The following figure displays the options for a set of Actions in the Simple Mode (FC).

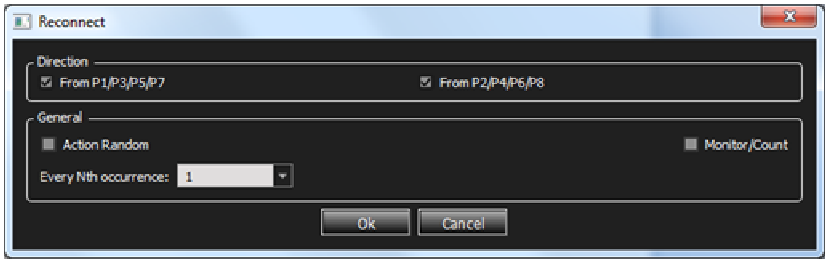


Action

Filter...

- User Actions
- Presets
  - Basic
    - Beep
    - Monitor/Count
    - Marker
    - Link Control
      - Reconnect
      - Disconnect
  - DWORD Jam
    - Replace DWORD
  - Symbol Jam
    - Replace With Another Symbol
    - Delete
  - Frame Jam
    - Insert Bytes Inside Frame
    - Modify
    - Replace
    - Remove[Replace With Idle]
    - Truncate
  - Inject General Error
    - FEC Parity Error
    - Sync Header Error
    - Invalid 10Bit Error Code
    - Running Disparity Error
  - Insert
    - New Frame
    - Symbol (66 Bit)
    - Bytes
  - Orderset Jam
    - Delete
    - Remove[Replace With Idle]
    - Replace With Another Orderset
  - Scenario Execution
    - Stop Scenario
    - Restart All Sequence
    - Restart Current Sequence
  - Training Sequence Jam
    - Modify
  - Branch To
    - Destination State
  - Trigger Output
    - Analyzer Trigger
    - External Trigger
    - Internal Trigger
  - Capture
    - DWORD

Figure 4.10: FC Action Properties Dialog



Reconnect

Direction

☑ From P1/P3/P5/P7 ☑ From P2/P4/P6/P8

General

□ Action Random □ Monitor/Count

Every Nth occurrence: 1

Figure 4.11: Reconnect Menu for Selecting Direction

The following table lists the supported Actions. Note that some of these Actions only apply to creating sequences.

TABLE 4.5: Test State Actions in Simple Mode

Action		Description
Basic	Beep	Emits audible sound of duration selectable via a drop-down list.
	Monitor Count	Opens a window to count the number of Events that occur during a session. A session is a time interval during which a Scenario runs.
	Link Control	Reconnect - starts traffic pass-through immediately. This Action restarts traffic after a previous disconnect command. Once traffic is passing through, the originator and responder resume link bring up. Disconnect - puts InFusion ports at electrical idle immediately. This action is only in effect while the scenario is running, and the Jammer will reconnect the line when the scenario is stopped.
		Reconnect/Disconnect can be applied in either direction separately: From P1/P3/P5/P7 direction: Reconnect/ Disconnect only the originator link. From P2/P4/P6/P8 direction: Reconnect/ Disconnect only the responder link. (See Figure 4.11 on page 188.)
DWORD Jam	Replace DWORD	Replace DWORD.
Symbol Jam	Replace with Another Symbol	Replaces the Symbol with the selected Symbol.
	Delete	Deletes the Symbol Jam.
Frame Jam	Insert Bytes Inside Frame	Allows to insert up to 60 Bytes inside the frame, at the specified offset or at the “current” dword, meaning the dword that caused the Event.
	Modify [Keep Length]	Allows to manipulate each dword in the header, with the selected Action (click on Pass though to get a drop-down list).
	Replace	Replaces the whole frame with the selected frame.
	Remove [Replace with IDLE]	Removes the whole frame.
	Truncate	Removes some of the payload, as specified in the Frame Length.

Action		Description
Inject General Error	FEC Parity Error	Injects a FEC error into traffic.
	Sync Header Error	Injects a Sync Header error into traffic.
	Invalid 10-bit-Error Code	Injects invalid 10b code into the line (FC8 only).
	Running Disparity Error	Injects a Running Disparity (RD) error into traffic(FC8 only).
Insert	Insert New Frame	Allows to insert a whole frame as specified from the list of available frames.
	Symbol (66 Bit)	Allows to insert a Symbol 66 bits.
	Insert Bytes	Allows to insert Bytes (FC 16 only).
Ordered Set Jam	Delete	Delete an Ordered Set Jam.
	Remove [Replace with IDLE]	Remove an Ordered Set Jam or Replace with another Ordered Set.
	Replace with Another Ordered Set	Only replace with another Ordered Set.
Scenario Execution	Stop Scenario	Stops the current Scenario. This Action should be the only Action in a State as it has higher priority over other Actions.
	Restart All Sequence	Restart all sequences in the Scenario.[1]
	Restart Current Sequence	Restart the sequence that contains this Action definition. [1]
Training Sequence Jam	Modify	Modify the Training Sequence Action Jam.
Branch To	Destination State	Go to a state in this Sequence.[1]
Trigger Output		Sends a signal out the trigger port to the device downstream.
	Analyzer Trigger	1. The Action is to send a trigger to the Analyzer. 2. The trigger point in the Analyzer that caused the analyzer trigger action will not be the selected event, it will be the selected event with some offset.
	External Trigger Output	The Action is to cause an external trigger output.
	Internal Trigger Output	The Action is to cause an internal trigger output.
	Marker Trigger	Add a marker to captured data.
Capture	DWORD	Capture DWORD.
		Reuse of Captured DWORDs. (See “Reusing “Captured DWORDS” in Events” on page 195.)

Action	Description
Jammer Internal Triggers	Refer to section "Synch Jammer Scenarios with Jammer Internal Triggers" on page 206.

[1] Only shown in Action Properties dialog box when creating a sequence.

4.6.5 Available Resources

You can specify Events, Combined Events and Actions and additional Events. The application automatically checks for the maximum number of terms (Events/Actions). When you exceed the limit, an error is flagged, prompting you to jump to the place that caused the error.

The list of available resources for Ethernet is given below:

- Symbol Detector(each has its own Embedded counter) X 4
- Auto-Neg Detector X 4
- Counter X 12
- Frame Detector X 8
- Timer X 8
- Frame Jammer X 8
- Symbol Substitute X 16
- Aut-Neg Jammer X 4
- Capture DWORD slot X 8
- Insert/Save frame slot (up to 16K bytes) X 7
- Insert BYTEs/Symbols inside frame (up to 128 bytes) X 8
- Global Action Register X 8
- State per sequencer X 256
- Action Register per state X 8

Usage of Action Register:

- Each Counter in Global Rules = 1
- Each Counter in State = 1
- Each Timer in Global Rules = 2
- Each Timer in State = 3
- Other Actions = 1

The list of available resources for Fibre Channel is given below:

- Symbol Detector (each has its own Embedded counter) X 4
- Ordered-set Detector (each has its own Embedded counter) X 8
- Pattern (32bit) Detector (each has its own Embedded counter) X 12
- Training Sequence Detector X 4
- Counter X 12
- Frame Detector X 8
- Timer X 8
- Frame Jammer X 8
- Symbol Substitute X 4

- ❑ Pattern/Orderded-set Substitute X 12 (shared with Pattern detectors)
- ❑ Training Sequence Jammer X 4
- ❑ Capture DWORD slot X 8
- ❑ Insert frame slot (up to 4K bytes) X 1
- ❑ Insert DWORD inside frame (up to 64 bytes) X 8
- ❑ Global Action Register X 8
- ❑ State per sequencer X 256
- ❑ Action Register per state X 8

Usage of Action Register:

- ❑ Each Counter in Global Rules = 2
- ❑ Each Counter in State = 3
- ❑ Each Timer in Global Rules = 2
- ❑ Each Timer in State = 3
- ❑ Other Actions = 1

4.6.6 Using Counters in Events and Actions

Many of the Events and Actions supported by InFusion also support counters that can control functions.

Within Events, counters determine how many times the Event must occur before the associated Actions are triggered. Event counters typically have two properties:

- ❑ **Count Randomly**: Can be set to “Yes” or “No” (default value is “No”).
  If the **Count Randomly** checkbox is selected, the Event repeats a random number of times (between 1 and the value set in the property **Max Random Count**, which replaces the property **Counter Value** when “Yes” is selected), before the Action is triggered.
- ❑ **Counter Value**: Number of repeats required when the **Count Randomly** checkbox is not selected. The default value is 1.

Within Actions, counters determine how many times the Event happens before it executes the Action. Note that an Event can be defined for a number of occurrences, so in total, the Event will have to occur for Event counter multiplied by the Action counter times before the Action gets executed. For example, if the Event is defined with a counter of 5, and Action with a counter of 10 such Events, the Event looked at will have to occur 50 times before the Action is taken.

Action counters typically have two properties:

- ❑ **Action Random**: Can be set to “Yes” or “No” (default value is “No”).
  If the **Action Random** checkbox is selected, the Action triggers a number of occurrences before the Action takes place. That number ranges randomly between 1 and the value set in the property **Every Nth occurrence**, which replaces the property **Every Nth occurrence** when the **Action Random** checkbox is selected.
- ❑ **Every Nth occurrence**: Number of times the system calls the Action before it acts.

Note that there is some overlap in the way these counters can be used. For example, in the simple case of a single Event leading to a single Action, it makes no difference whether you specify the Event to require five repeats before triggering the Action, or the Action to require five occurrences before it acts.

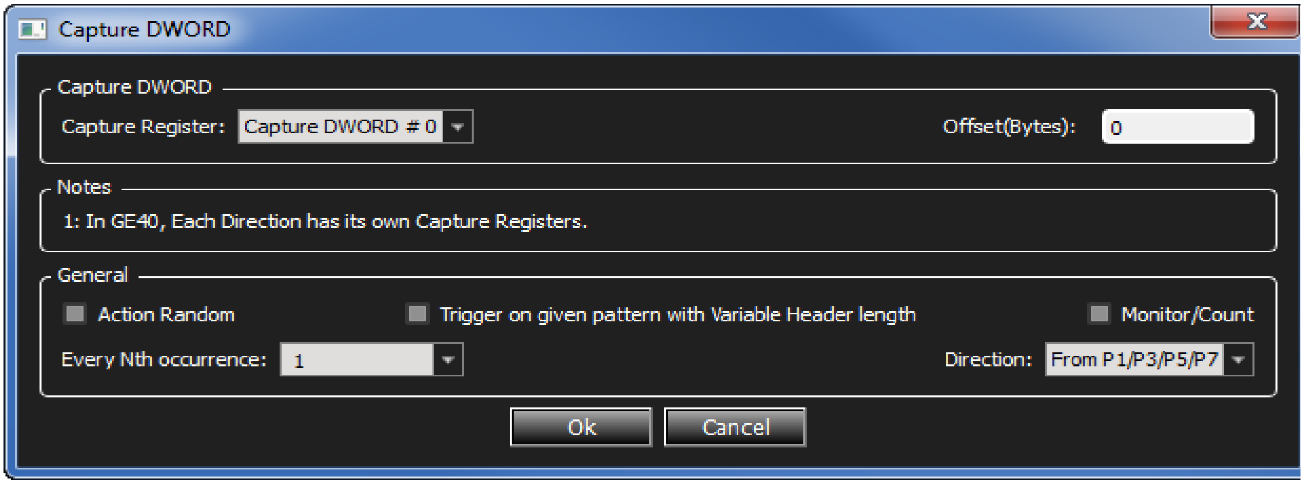
However, in the case of combined Events and/or Actions, the separate counters provide flexibility in designing test cases. For example, consider the case where Event_1 OR Event_2 leads to Action. If Event_1 has a counter of 5, then the Action triggers either when Event_1 has repeated five times or when Event_2 happens the first time, whichever occurs first.

But if the Event counters are set to 1 and the Action counter is set to 5, then the Action happens after five occurrences of EITHER Event_1 or Event_2.

4.6.7 Capturing a Data Dword

InFusion provides the ability to capture individual data dwords and provides different registers to store captured dwords. When your detector is DWord Matcher you can use Dword #0, #1, #2 and #3 and when your detector is Pattern Detector you can use Dword #4, #5, #6 and #7. When trying to use the captured dword, for example in Replace Dword Action, you can actually select from 8 captured dwords, numbered 0 through 7.

To capture a data dword, select **Capture Dword** from the Action Properties screen (see Figure 4.12 on page 193). Select the location you would like the captured Dword to be stored in, so it can be used in a later replacement or insertion.



Capture Register: Capture DWORD # 0

Offset(Bytes): 0

1: In GE40, Each Direction has its own Capture Registers.

Every Nth occurrence: 1

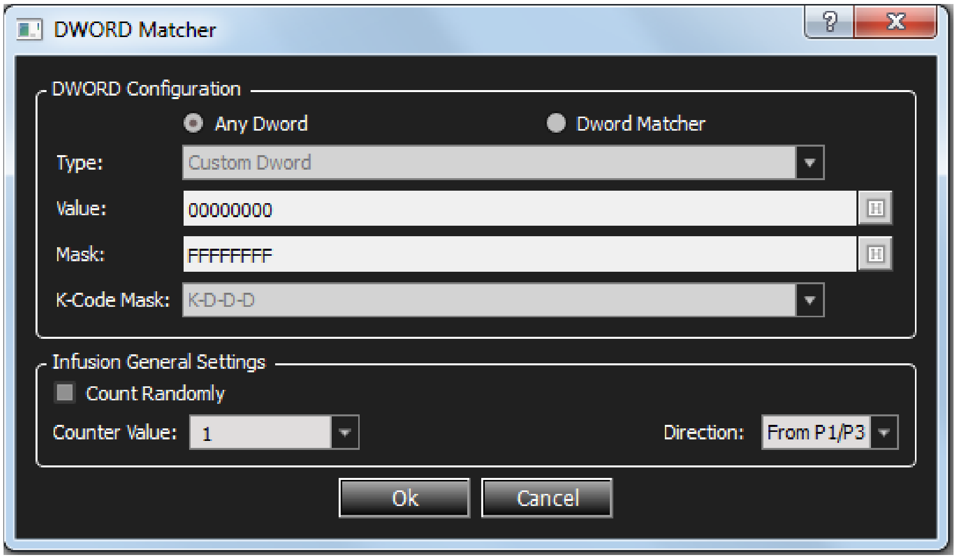
Direction: From P1/P3/P5/P7

Figure 4.12: Capture Data Dword Action

4.6.8 Using Captured Data Dwords

Captured data dwords can be used in creating Events for data that match the captured dword(s), or in creating Actions to substitute or insert the captured dword(s) into the data stream.

To create an Event using the captured dword, in the Add Event dialog (see Figure 4.13 on page 194), select Dword Matcher and change the Type to the desired Captured Dword number. Note that choice of a mask and an offset are still available. Select the code mask from the drop-down menu.



DWORD Matcher

DWORD Configuration

○ Any Dword ● Dword Matcher

Type: Custom Dword

Value: 00000000

Mask: FFFFFFFF

K-Code Mask: K-D-D-D

Infusion General Settings

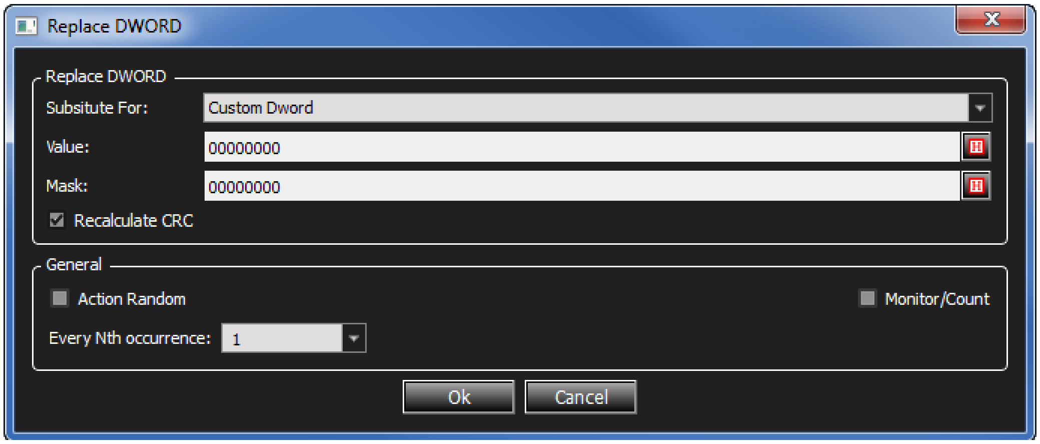
□ Count Randomly

Counter Value: 1

Direction: From P1/P3

Figure 4.13: Using Captured Dword as an Event

Captured data dwords may also be used in the **Substitute Data Dword** Action. From the Action Properties screen, click on the **DWORD Jam** icon and click on Replace DWORD, choose **Substitute For Custom Dword** and then select the **Substitute for** property. A drop-down menu is provided (see below) that allows the choice of a custom dword or any of the four captured dword registers.



Replace DWORD

Replace DWORD

Subsitute For: Custom Dword

Value: 00000000

Mask: 00000000

☑ Recalculate CRC

General

□ Action Random □ Monitor/Count

Every Nth occurrence: 1

Figure 4.14: Using a Captured Data Dword in Substitute Dword Test Action

4.6.9 Dword Matcher

Dword Matcher is a dword pattern matcher that presents match and mask fields and a K-Code Mask field. K-Codes are control characters that are always used in the first byte of a four-byte ordered-set. Of the K-Code masks listed in the menu, D-D-D-D is used for data bytes, and K-D-D-D is used for all ordered-sets.

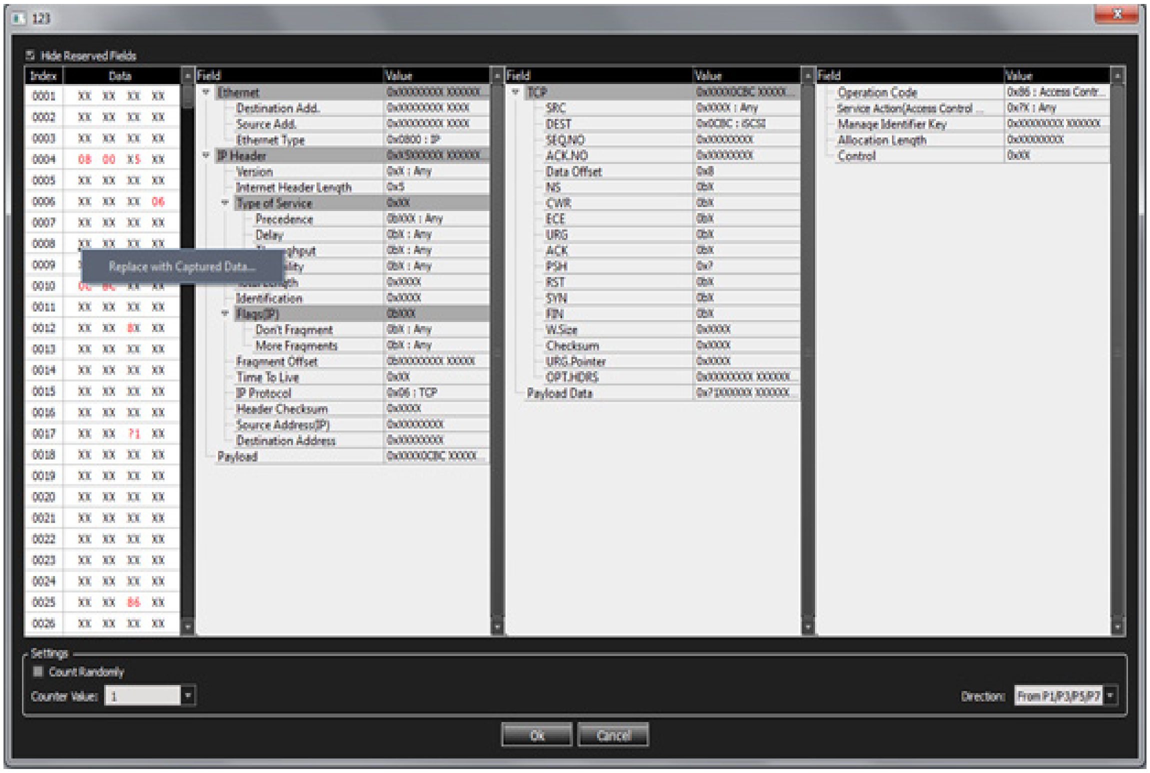
When you create a dword match, keep the following in mind:

- ❑ The pattern can be inside or outside of frames (it does not matter if the pattern is inside a frame or not).
- ❑ Because the pattern can be inside or outside of frames, there is no offset.
- ❑ You can make user-defined ordered-sets. (This is the reason this feature was created.)
- ❑ You can use any K/D pattern.

4.6.10 Reusing “Captured DWORDS” in Events

This feature will enable the user to reuse previously captured data inside a Frame event; therefore some parts of the frame event can be changed during the jammer running period in real time.

To use a captured DWord in a Frame Event, the user can right click on Data pane of the Frame Event Properties dialog and choose “Replace with Captured DWord”. Then another dialog will pop up and the user can specify which captured DWord (Capture DWord#0 to Capture DWord#3) to use to replace the selected DWord at run time. A user can mask any of the bytes of the captured DWord by using the Mask buttons provided in the “Replace With Captured Data” dialog.

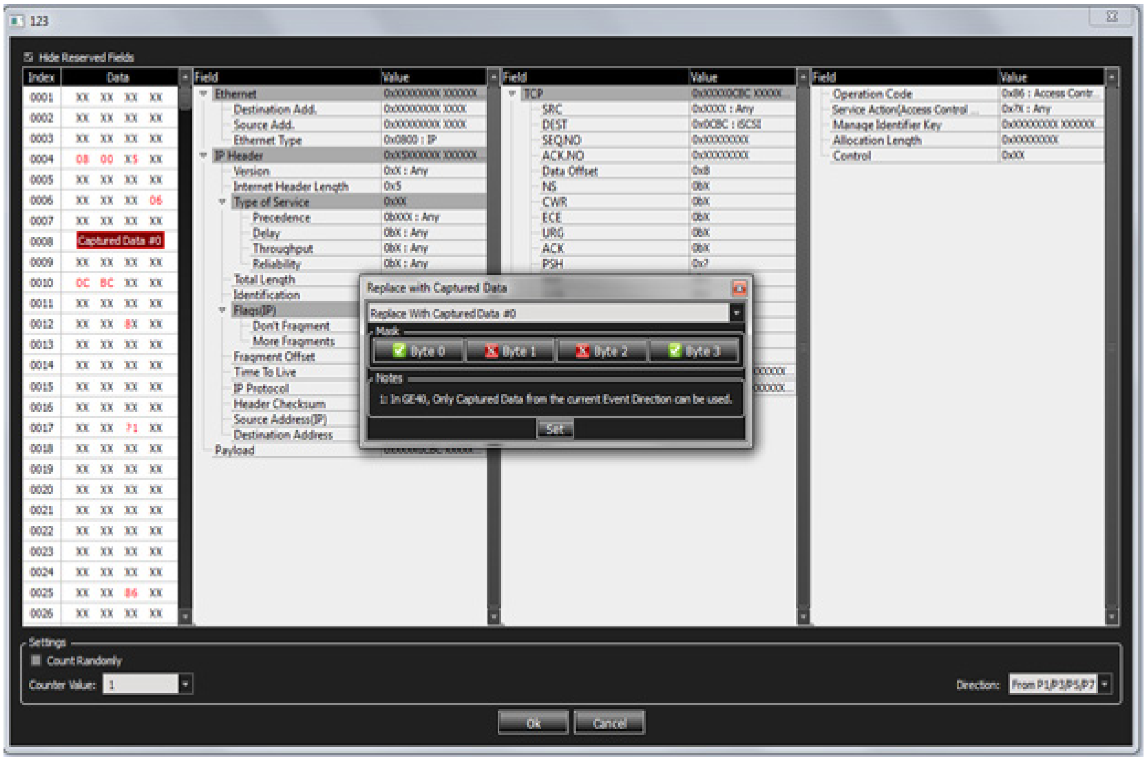


Field	Value
Ethernet	0x00000000000 XXXXXX
Destination Add.	0x00000000000 XXXX
Source Add.	0x00000000000 XXXX
Ethernet Type	0x0800 : IP
IP Header	0xX5X00000X XXXXXX
Version	0xX : Any
Internet Header Length	0x5
Type of Service	0xXX
Precedence	0bXXX : Any
Delay	0bX : Any
Throughput	0bX : Any
Reliability	0bX : Any
Total Length	0xXXXX
Identification	0xXXXX
Flags(IP)	0bXXX
Don't Fragment	0bX : Any
More Fragments	0bX : Any
Fragment Offset	0bXXXXXXXXX XXXXXX
Time To Live	0xXX
IP Protocol	0x06 : TCP
Header Checksum	0xXXXX
Source Address(IP)	0xXXXXXXXX
Destination Address	0xXXXXXXXX
Payload	0xXXXXX0CBC XXXXXX

Field	Value
TCP	0xXXXX0CBC XXXXXX
SRC	0xXXXX : Any
DEST	0x0CBC : iSCSI
SEQ.NO	0xXXXXXXXX
ACK.NO	0xXXXXXXXX
Data Offset	0x8
NS	0bX
CWR	0bX
ECE	0bX
URG	0bX
ACK	0bX
PSH	0x?
RST	0bX
SYN	0bX
FIN	0bX
W.Size	0xXXXX
Checksum	0xXXXX
URG.Pointer	0xXXXX
OPT.HDRS	0xXXXXXXXXX XXXXXX
Payload Data	0x?1XXXXXX XXXXXX

Field	Value
Operation Code	0x86 : Access Contr...
Service Action(Access Control ...	0x?X : Any
Manage Identifier Key	0xXXXXXXXXX XXXXXX
Allocation Length	0xXXXXXXXX
Control	0xXX

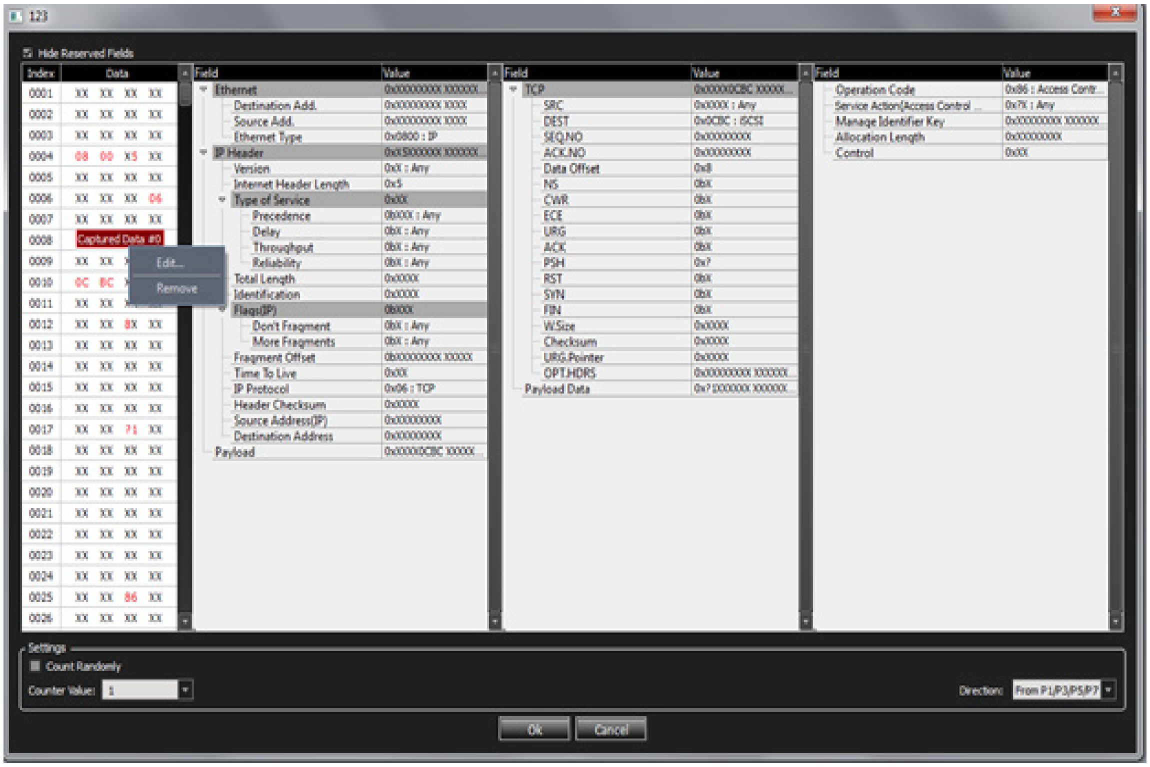
Figure 4.15: Replace with Captured DWORD Menu



1: In GE40, Only Captured Data from the current Event Direction can be used.

Figure 4.16: Replace with Captured Data Dialog

To remove or edit the existing captured DWord in an event, the user can right-click on the desired DWORD and choose “Remove” or “Edit”



Index	Data
0001	XX XX XX XX
0002	XX XX XX XX
0003	XX XX XX XX
0004	08 00 X5 XX
0005	XX XX XX XX
0006	XX XX XX 06
0007	XX XX XX XX
0008	Captured Data #0
0009	XX XX X
0010	0C BC X
0011	XX XX X
0012	XX XX 8X XX
0013	XX XX XX XX
0014	XX XX XX XX
0015	XX XX XX XX
0016	XX XX XX XX
0017	XX XX 71 XX
0018	XX XX XX XX
0019	XX XX XX XX
0020	XX XX XX XX
0021	XX XX XX XX
0022	XX XX XX XX
0023	XX XX XX XX
0024	XX XX XX XX
0025	XX XX 86 XX
0026	XX XX XX XX

Field	Value
Ethernet	0xXXXXXXXXXX XXXXXX...
Destination Add.	0xXXXXXXXXXX XXXX
Source Add.	0xXXXXXXXXXX XXXX
Ethernet Type	0x0800 : IP
IP Header	0xX5XXXXXX XXXXXX...
Version	0xX : Any
Internet Header Length	0x5
Type of Service	0xXX
Precedence	0bXXX : Any
Delay	0bX : Any
Throughput	0bX : Any
Reliability	0bX : Any
Total Length	0xXXXX
Identification	0xXXXX
Flags(IP)	0bXXX
Don't Fragment	0bX : Any
More Fragments	0bX : Any
Fragment Offset	0bXXXXXXXXX XXXXX
Time To Live	0xXX
IP Protocol	0x06 : TCP
Header Checksum	0xXXXX
Source Address(IP)	0xXXXXXXXX
Destination Address	0xXXXXXXXX
Payload	0xXXXX0CBC XXXXX

Field	Value
TCP	0xXXXX0CBC XXXXX...
SRC	0xXXXX : Any
DEST	0x0CBC : iSCSI
SEQ.NO	0xXXXXXXXX
ACK.NO	0xXXXXXXXX
Data Offset	0x8
NS	0bX
CWR	0bX
ECE	0bX
URG	0bX
ACK	0bX
PSH	0x?
RST	0bX
SYN	0bX
FIN	0bX
W.Size	0xXXXX
Checksum	0xXXXX
URG.Pointer	0xXXXX
OPT.HDRS	0xXXXXXXXXX XXXXXX...
Payload Data	0x?1XXXXXX XXXXXX...

Field	Value
Operation Code	0x86 : Access Contr...
Service Action(Access Control ...	0x?X : Any
Manage Identifier Key	0xXXXXXXXXX XXXXXX...
Allocation Length	0xXXXXXXXX
Control	0xXX

☐ Count Randomly

Counter Value: 1

Direction: From P1/P3/P5/P7

Figure 4.17: Remove or Edit Captured DWORD

4.6.11 Global Rules

Global Rules are a portion of the Scenario that can define only one test state. To create the Global Rules, you use the menu-driven interface to enter an Event or Combined Event and the corresponding Action or set of Actions (the response of InFusion hardware to the Event).

In the case of a Combined Event, the Action is taken upon occurrence of any of the Events stated for the Event combination. It is a logical OR association, meaning any of the Events can trigger the Action.

After you enter the Event or Combined Event, the interface prompts you for Actions. An Action might be, for example, injecting a particular ordered-set or error into the traffic stream. You can enter multiple Actions, which take place simultaneously. If one of the Actions is Stop Scenario, the other Actions will NOT be carried out. To stop the Scenario after the requested Actions have been carried out, you should branch to a new state which stops the Scenario.

After defining the Event and Actions within the Global Rules panel, you can save the Scenario and run it.

4.6.12 Sequences

The Global Rules are all you need for simple test Scenarios. However, a Scenario also can contain one or two sequences, which can define multiple states and allow branching between states. With a sequence, you also can do looping, which allows you to repeat a test state or to execute a test for a specified period of time.

As with Global Rules, the menu-driven interface guides you in building a sequence. Some of the prompts are different, however, because you now are encapsulating groups of Events and Actions as distinct states. Recall that a state is a combination of Events and Actions at a specific point in time. If the Event or Combined Event defined by a state occurs, the corresponding Action or set of Actions follows. You can enter multiple Actions, which take place simultaneously. If one of the Actions is Stop Scenario, the other Actions are carried out. To stop the Scenario after the requested Actions have been carried out, you should branch to a new state which stops the Scenario.

InFusion hardware provides the capacity to have up to two sequences co-existing in a Scenario in addition to the Global Rules. Recall that both the Global Rules and any sequences are active at all times. Each is a separate “state machine,” having the behavior of a particular test state at any point in time. Because the Global Rules has the capacity for only one state, you can view it as a “degenerative state machine.”

4.6.13 Scenario Libraries

Libraries are repositories that hold Scenarios. This section describes the ways that you can manipulate Scenarios within Libraries.

Scenario Library Item Multi-Selection

The Scenario Library lists support conventional multi-selection via mouse-clicks and keyboard modifiers. The Copy Scenario item from the right-click context menu will operate on all selected items:

- ❑ Hold down the Ctrl key on the keyboard and click on items to toggle their selection state.
- ❑ Select a first item, then hold down the Shift key and select a second item; all items from the first item to the second item will be selected.

Global and Project Libraries

The scenarios saved in the Global Library are available to reuse for all projects. The scenarios saved in the Project Library are only available for the current project. You may transfer Scenarios between these libraries by drag-n-drop or copy/paste.

Adding Scenarios from Global to Project can only work if the protocol is similar, else it will be greyed out and unselectable.

Import/Export of Scenarios

Users can export a scenario (or multiple scenarios) to a file. Export is available via right click pop up menu. Scenarios can then be archived on your host machine’s hard drive.

There are two ways to import a library, if the user wants to import file into a existing library, they have to right click on the existing library and select import library. If the user wants to make a new library, there is an icon to import a library in library pane toolbar.

4.6.14 Traffic Direction

The direction for traffic modification is defined on a global basis for the entire Scenario. In other words, any Scenario Action that modifies line traffic only affects the traffic flowing in the direction established at the top of the Scenario, in the Scenario Properties. Scenario Events can be monitored in either direction, and therefore the parameters for Events provide the ability to specify the intended direction for monitoring traffic for that Event.

You identify direction of traffic change, or modification, in terms of traffic origin. The application uses the following conventions:

- ❑ **From P1/P3**: Change is made to traffic coming from Port 1 or Port 3 (for example, CRC error is injected into traffic stream sent from P1/P3 to P2/P4).
- ❑ **From P2/P4**: Modification is made to traffic coming from the Port 2 or Port 4 (for example, CRC error is injected into traffic stream sent from P2/P4 to P1/P3).

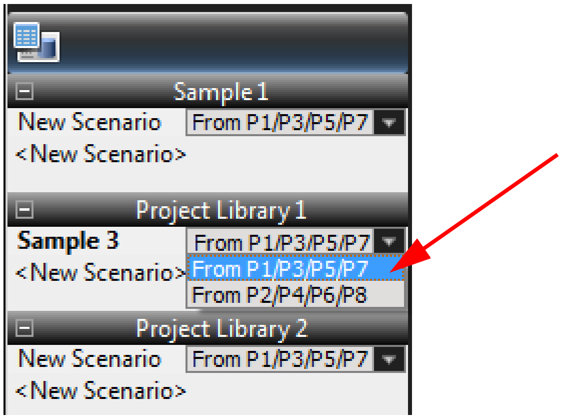


Figure 4.18: Traffic Direction

To copy an Event or Action, right-click on the Event or Action and select **Copy**. Right-click and select **Paste**.

You can also remove, cut and copy a selected Event or Action.

You can double-click the State name and edit it.

4.6.15 Copy and Paste Scenarios

You can copy and paste scenarios from one project to another project. Perform the following steps to do so:

1. Select the scenario you want to copy in either the scenario name tab and select **Copy** or in the Library pane, right-click and select **Copy Scenario** (see Figure 4.19 on page 200.

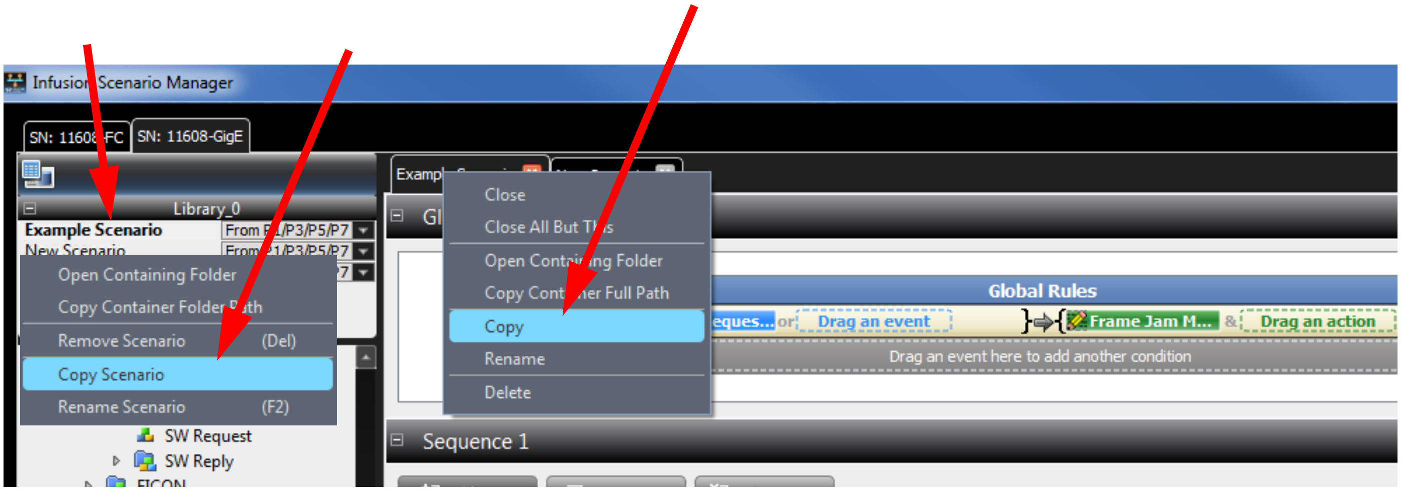


Figure 4.19: Copy Scenario

2. Place the cursor in the area below <New Scenario> in the Library pane, in the project you want to paste in, right- click and select **Paste Scenario**.

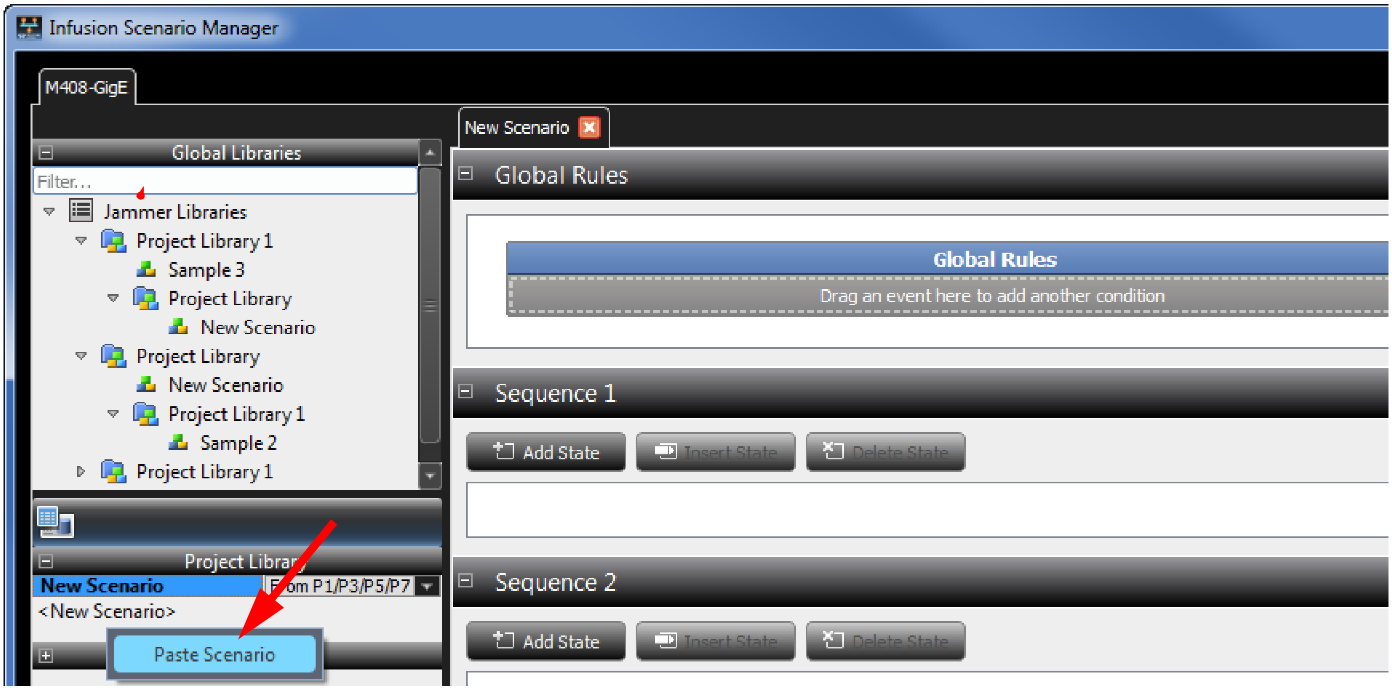


Figure 4.20: Paste Scenario

4.6.16 Copy and Paste Library

You can copy and paste libraries from one project to another project. Perform the following steps to do so:

1. Select the library you want to copy, right-click and select **Copy Library**.

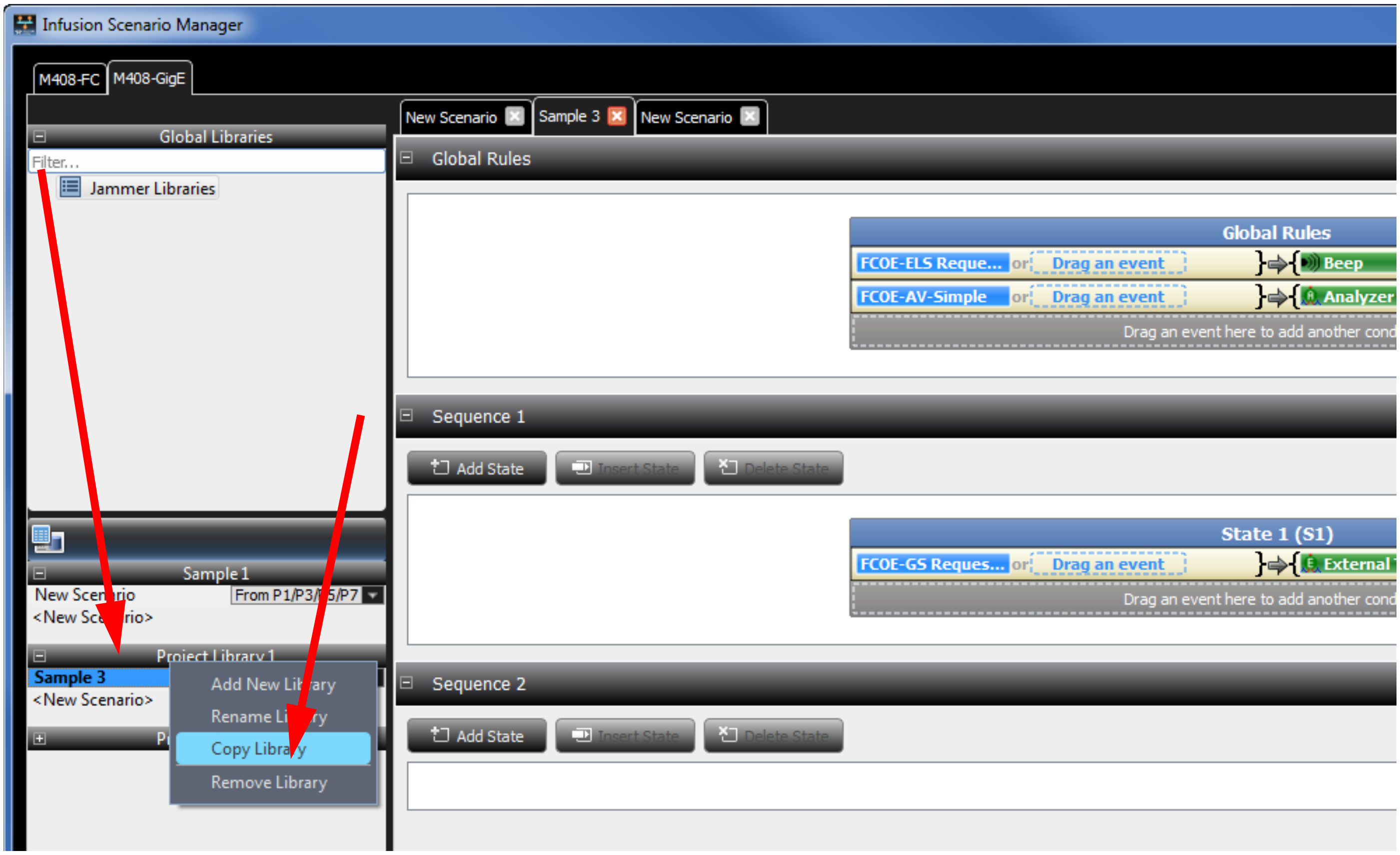


Figure 4.21: Copy Library

2. Place the cursor on the Jammer libraries icon in the Global Libraries panel, right-click and select **Paste**.

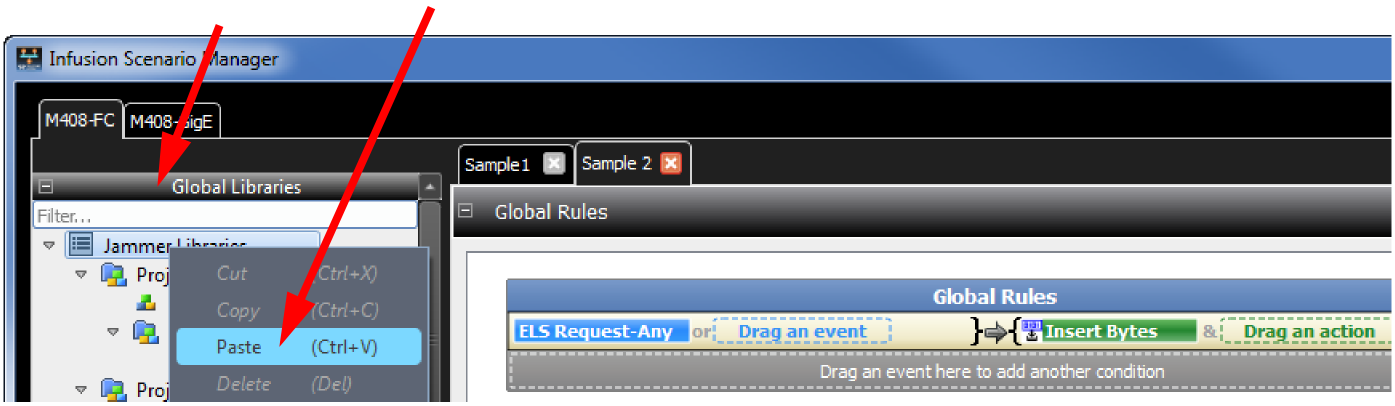


Figure 4.22: Paste Library

4.6.17 Copy/Cut and Paste States

You can copy and paste states from Global Rules to Sequences. You can also copy/cut and paste states between Sequences. You cannot cut a state from nor paste a state into Global Rules.

1. Right-click in the blue title area of the State you want to copy and select Copy State (or Cut State if applicable).
2. Right-click in the white workspace of the desired target Sequence and select Paste State.

4.6.18 Copy/Cut and Paste Conditions

You can copy and paste Conditions within and between States.

1. Right-click in the empty yellow space of the Condition you want to copy and select Copy Condition (or Cut Condition if applicable).
2. Right-click in the gray placeholder area (i.e. in the area that says "Drag an event here....") of the desired target State and select Paste.

4.6.19 Copy/Cut and Paste Events

You can copy and paste Events within and between States.

1. Right-click on the Event you want to copy and select Copy (or Cut if applicable).
2. Right-click in the empty yellow space of the desired target Condition or in the gray placeholder area (i.e. in the area that says "Drag an event here....") of the desired target State and select Paste.

4.6.20 Marker Trigger

Purpose

The main purpose of this feature is enabling the user to mark specific parts of the captured traffic for better tracking.

Solution

The Marker Trigger action will be added to Jammer under Trigger Output category. Also, for differentiating various markers, the action will has an Index parameter that will be shown in the captured traffic as well. Therefore 8 Marker actions will be as bellow:

1. Jammer Marker 1
2. Jammer Marker 2
3. Jammer Marker 3
4. Jammer Marker 4
5. Jammer Marker 5
6. Jammer Marker 6
7. Jammer Marker 7

8. Jammer Marker 8

Adding above markers can be used as an action in the Jammer. When the Jammer runs this action, the result is adding a marker (bookmark) in captured trace in analyzer. The added markers will be shown as a normal marker (bookmark) in trace and you can see list of marker in book mark dialog.

Note: The limitation for adding markers is 10,000, it means you can add up to 10,000 marker to a trace.

GUI

Marker trigger added under “Trigger output” node in action tree as below:

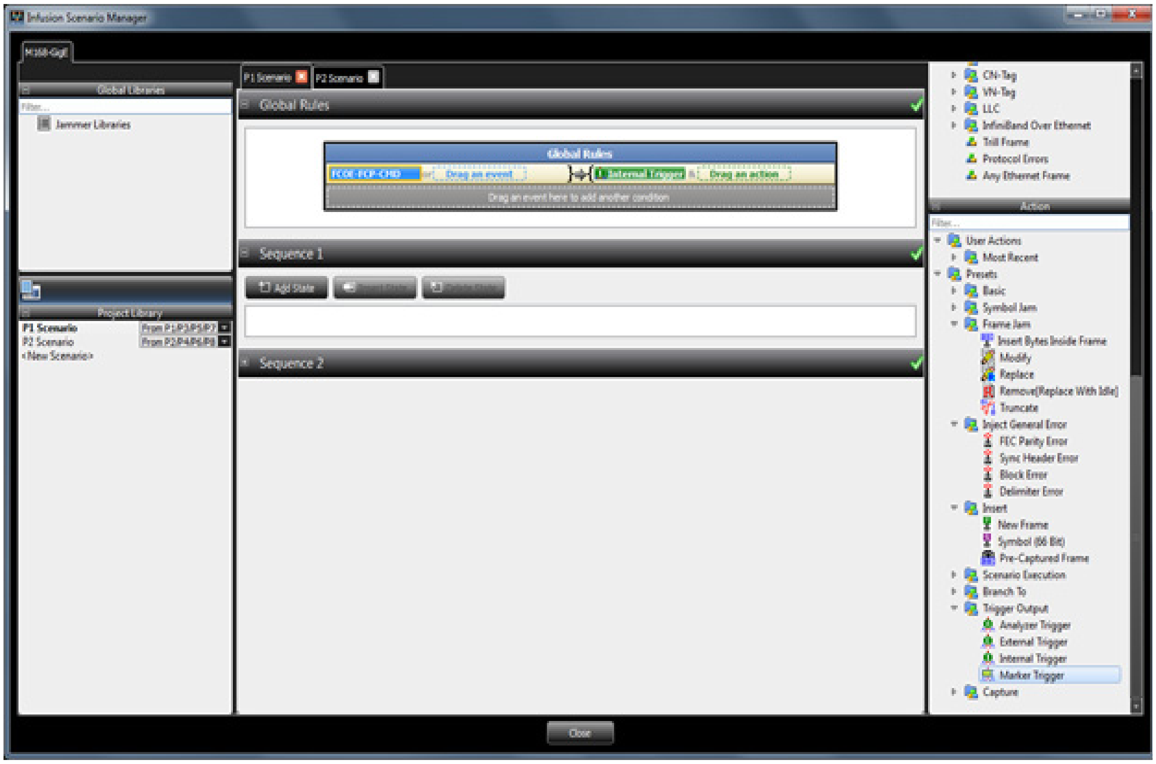
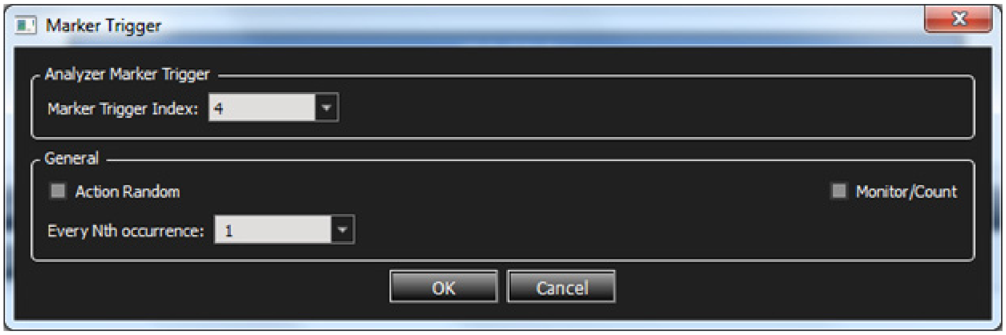


Figure 4.23: Marker Trigger Added to Action Tree

There is a dropdown list in Marker Trigger dialog to choose which marker user wants to insert to analyzer trace. (Marker 1 to Marker 8).



Marker Trigger Index: 4

□ Action Random

□ Monitor/Count

Every Nth occurrence: 1

Figure 4.24: Marker Trigger Menu

4.6.21 Synch Jammer Scenarios with Jammer Internal Triggers

By design, each Jammer port pair runs its own independent scenario, and each one can be controlled independently. However, there may be advanced cases where you would need to synchronize the Jammer operation of 2 or more port pairs. For example, you might want to create a setup in which you jam both directions of a single link; you can achieve this by looping the link through P1/P2 and P3/P4 with external cabling, running separate scenarios on each of P1/P2 and P3/P4, and synchronizing those scenarios with the Jammer Internal Triggers.

Jammer Internal Triggers are pairs of events and actions that enable cross-port signaling; these events and actions are manipulated like any other event and action. The Internal Trigger Action allows one port pair to signal an Internal Trigger Event on a different port pair. Note that the Internal Trigger Action will NOT signal an Internal Trigger Event on the same port pair. There are four independent Jammer Internal Trigger event/action pairs available

For supporting this feature, a specific signal between different paths should be added, such that one scenario will be able to notify the scenarios of other paths.

Thus, firstly, it is needed to add a new Action for notifying other paths and secondly, adding a new event for waiting on any notify signal that is raised on other paths. This will be implemented as bellow:

1. Adding ‘Internal Trigger’ action to notify all other paths :
   a. Internal Trigger Action 1
   b. Internal Trigger Action 2
   c. Internal Trigger Action 3
   d. Internal Trigger Action 4
2. Adding ‘Internal Trigger’ event to wait for others’ notifications
   a. Internal Trigger Event 1 which is corresponded to Internal Trigger Action 1
   b. Internal Trigger Event 2 which is corresponded to Internal Trigger Action 2
   c. Internal Trigger Event 3 which is corresponded to Internal Trigger Action 3
   d. Internal Trigger Event 4 which is corresponded to Internal Trigger Action 4

Example

For example, the user would like to insert a new frame on P1/P2 path (ACTION1) when there is a specific symbol on P3/P4 path (EVENT1), this scenario will be implemented in 2 different scenarios as below:

1. In the first scenario for P1/P2, in the global state define a condition that waits for EVENT1 and then raise ‘Internal Trigger’ action.
2. In the second scenario for P3/P4, in the global state define a condition that waits for the same ‘Internal Trigger’ event and the does ACTION1.

Scenario 1

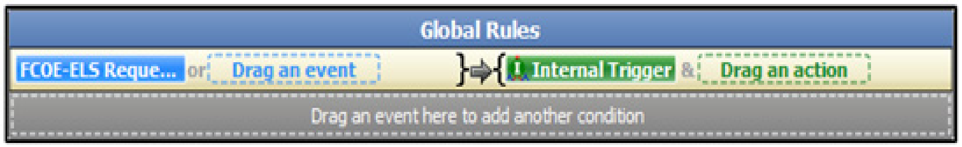


Figure 4.25: Scenario 1 using Jammer Internal Trigger

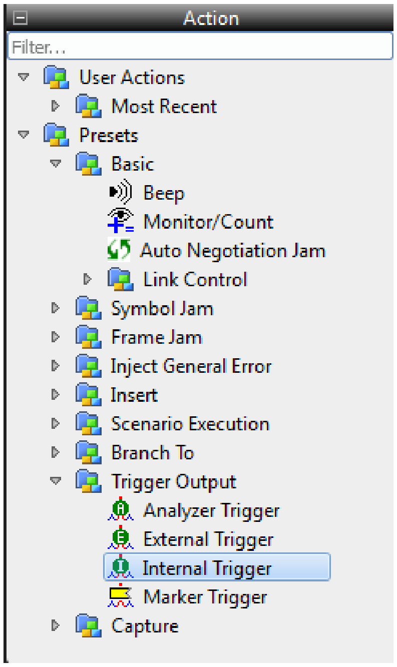
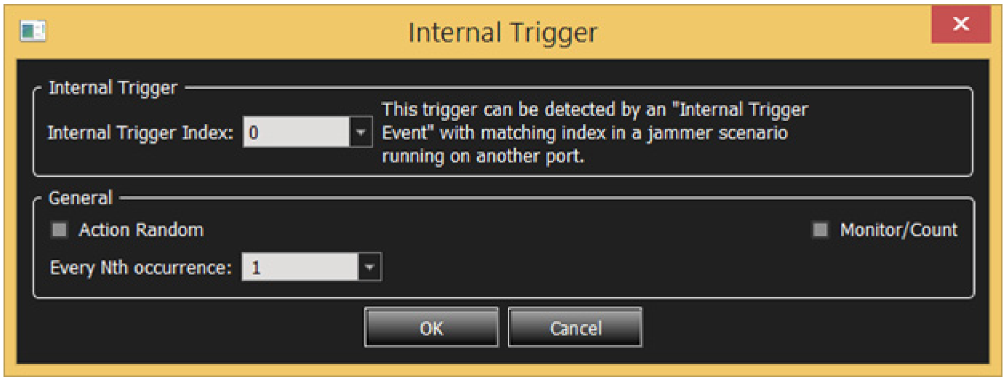


Figure 4.26: Internal Trigger action in the Actions pane


Internal Trigger

Internal Trigger

Internal Trigger Index: 0

This trigger can be detected by an "Internal Trigger Event" with matching index in a jammer scenario running on another port.

General

□ Action Random

□ Monitor/Count

Every Nth occurrence: 1

Figure 4.27: Internal Trigger Action Properties

Scenario 2

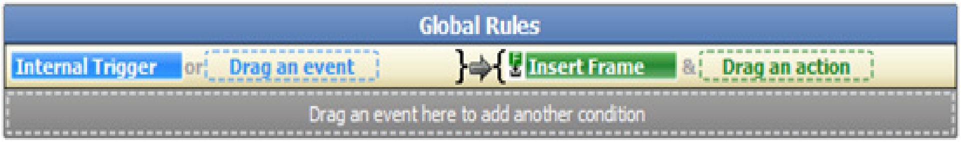


Figure 4.28: Scenario 2 using Jammer Internal Trigger Event

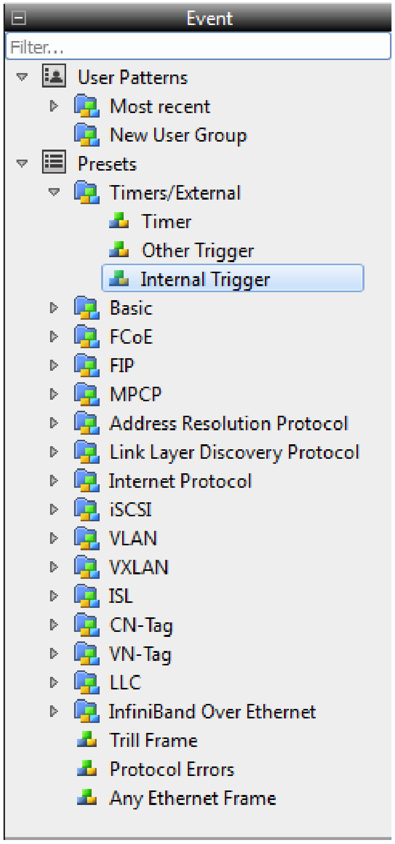
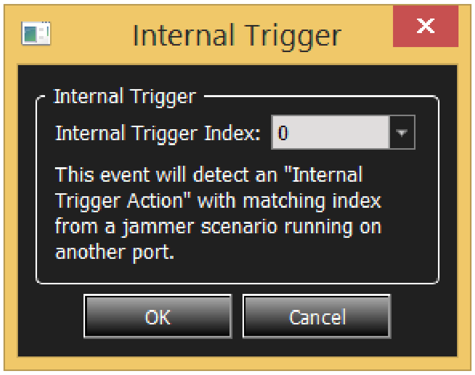


Figure 4.29: Internal Trigger Event in the Events Pane



Internal Trigger Index: 0

This event will detect an "Internal Trigger Action" with matching index from a jammer scenario running on another port.

Figure 4.30: Internal Trigger Event Properties

4.7 Scenario Example

4.7.1 Example: Insert DWORD Matcher

In this example, the Global Rules panel of the Scenario waits for a Custom Frame then inserts a Dword inside the frame. In Sequence 0 and State 0 it waits for an FCP SCSI Command, SBC3; inserts a Dword inside the frame, beeps for a duration of 50 ms and stops the Scenario.

Creating Global Rules

This section describes using the Global Rules panel of the Scenario for this example. Recall that the Global Rules panel defines a single test state. The Global Rules do not have the capacity for multiple states, so that area of a Scenario cannot change state.

In terms of InFusion testing, a state defines test “behavior.” In this context, behavior is “waiting” for an Event and responding with an Action or set of Actions that happen simultaneously.

Keep in mind that a test state you implement with the Global Rules operates in parallel with the active test state of each sequence in the Scenario.

In effect, InFusion lets you do up to three line tests at the same time. You can do one test with the Global Rules and a separate test with each sequence you create. You can have up to two sequences in a Scenario.

1. Select Traffic Direction from the drop-down list to trigger on the defined event or trigger from InFusion Jammer (the default is **From P1/P3**, which is selected for this example).
2. In the Global Rules panel (see Figure 4.31 on page 210).
3. Select **DWORD Matcher** in the Event panel and place it in the Global Rules panel (see Figure 4.32 on page 210).

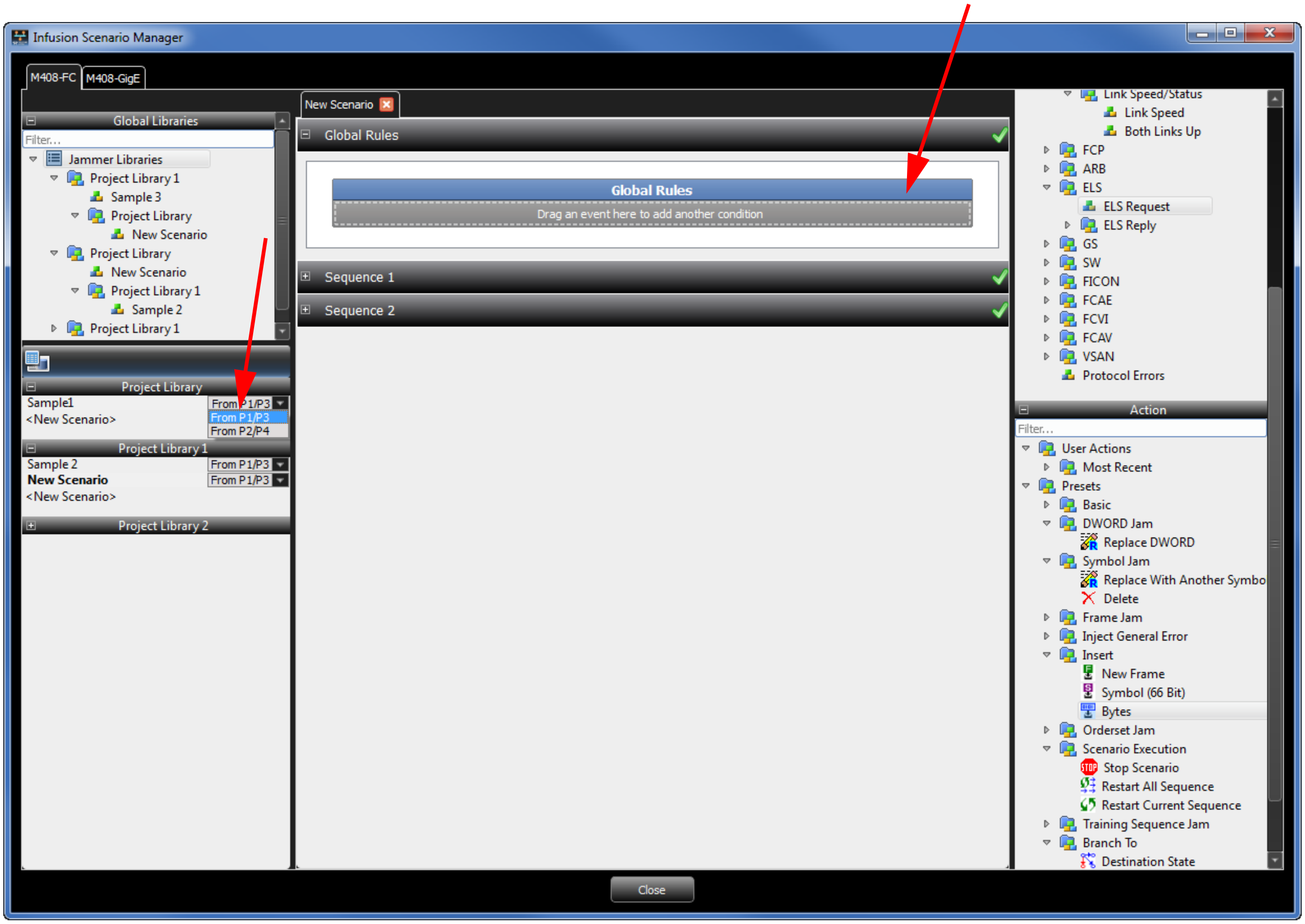
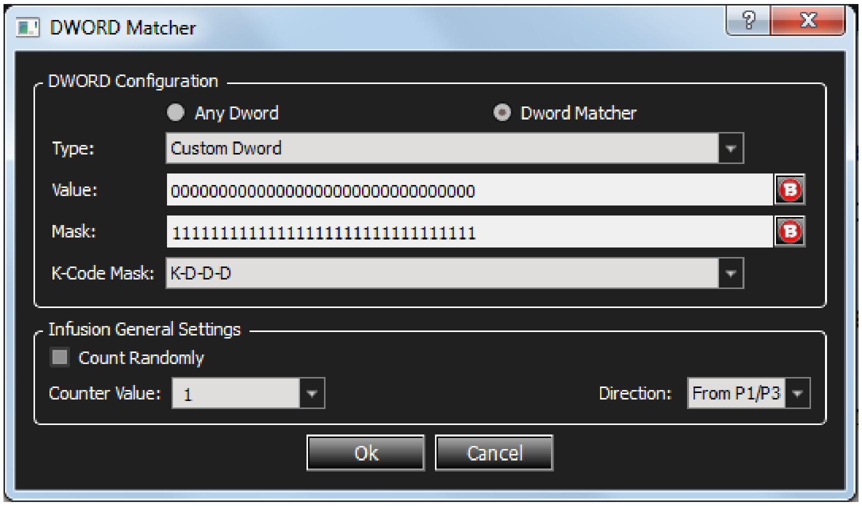


Figure 4.31: Global Rules Panel



DWORD Configuration

○ Any Dword ● Dword Matcher

Type: Custom Dword

Value: 00000000000000000000000000000000

Mask: 11111111111111111111111111111111

K-Code Mask: K-D-D-D

Infusion General Settings

□ Count Randomly

Counter Value: 1

Direction: From P1/P3

Figure 4.32: Adding an Event

4. The Event is added to the Global Rules panel (see Figure 4.33 on page 211).

5. Select **Replace DWORD** in the Action panel and place it in the Global Rules panel (see Figure 4.33 on page 211).
6. Right-click the New Scenario tab and select **Rename Scenario** and enter the name in the Library panel as shown in Figure 4.33 on page 211

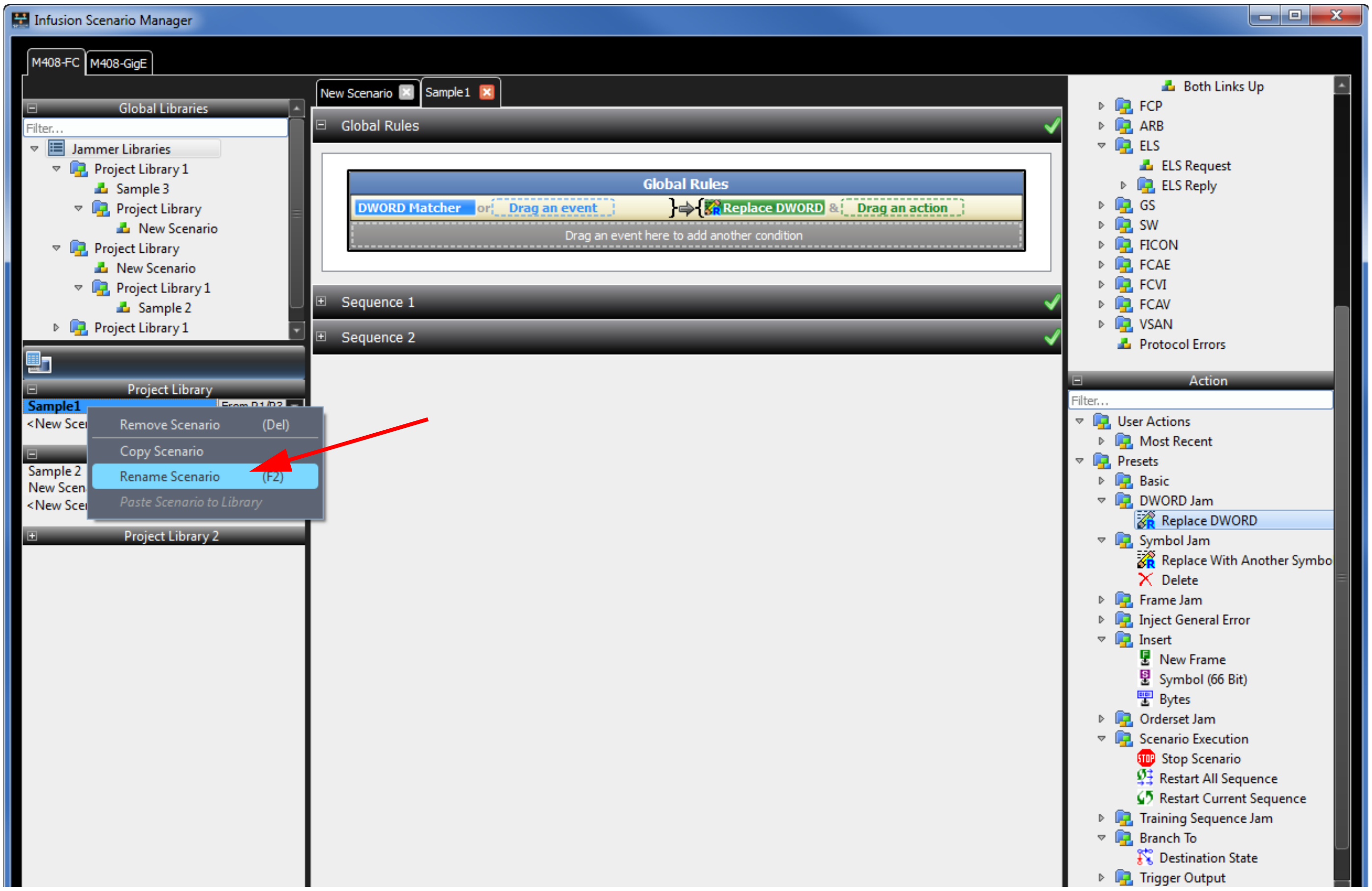


Figure 4.33: Global Rules - Naming a Scenario

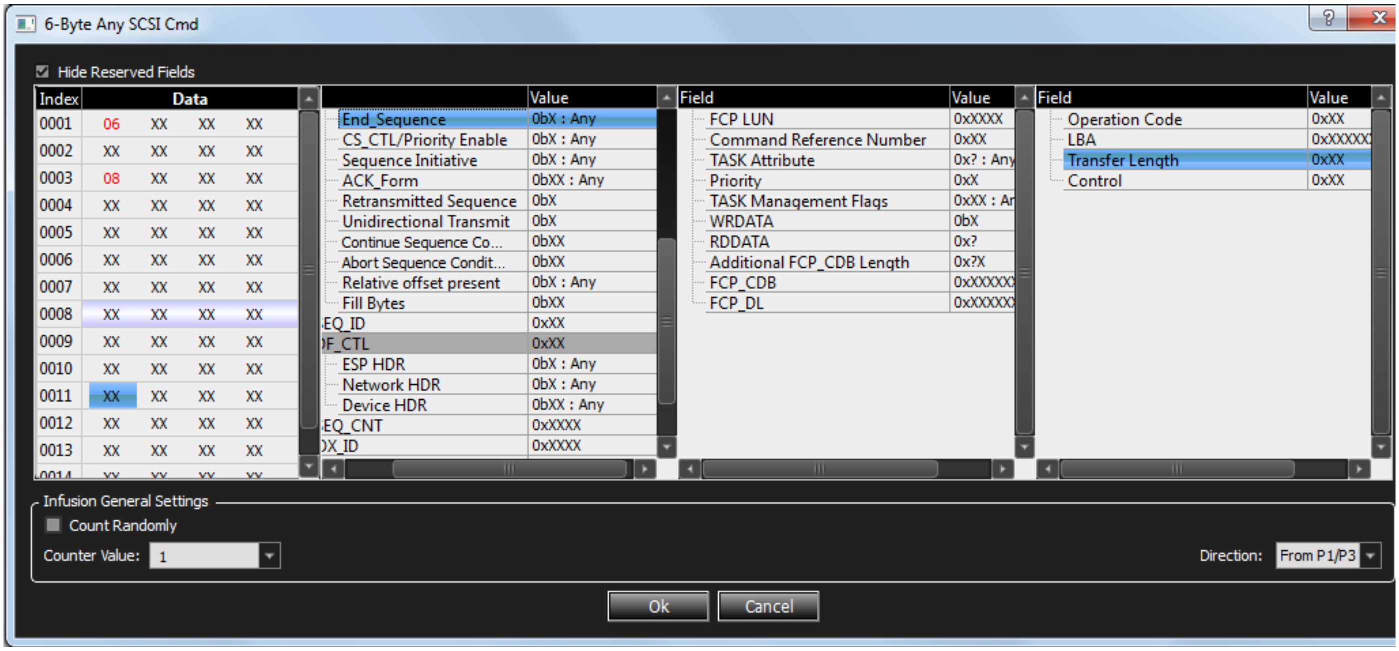
Adding a Sequence

To add a Sequence click **Add State in the Sequence 1** panel.

You create a sequence one state at a time. The application numbers states consecutively from 0 up (1, 2, 3, and so on).

By default, the name of the first sequence in a Scenario is Sequence 1. The name of the first state is State 0. To change the name of a sequence or state, or to associate a description with it, click the name of the sequence or state..

1. Drag **6-Byte Any SCSI Command** under **FCP** as the Event to display the dialog.



6-Byte Any SCSI Cmd

☑ Hide Reserved Fields

Index	Data			
0001	06	XX	XX	XX
0002	XX	XX	XX	XX
0003	08	XX	XX	XX
0004	XX	XX	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	XX	XX	XX	XX
0009	XX	XX	XX	XX
0010	XX	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX

	Value
End_Sequence	0bX : Any
CS_CTL/Priority Enable	0bX : Any
Sequence Initiative	0bX : Any
ACK_Form	0bXX : Any
Retransmitted Sequence	0bX
Unidirectional Transmit	0bX
Continue Sequence Co...	0bXX
Abort Sequence Condit...	0bXX
Relative offset present	0bX : Any
Fill Bytes	0bXX
EQ_ID	0xXX
F_CTL	0xXX
ESP HDR	0bX : Any
Network HDR	0bX : Any
Device HDR	0bXX : Any
EQ_CNT	0xXXXX
X_ID	0xXXXX

Field	Value
FCP LUN	0xXXXX
Command Reference Number	0xXX
TASK Attribute	0x? : Any
Priority	0xX
TASK Management Flags	0xXX : Ar
WRDATA	0bX
RDDATA	0x?
Additional FCP_CDB Length	0x?X
FCP_CDB	0xXXXXXX
FCP_DL	0xXXXXXX

Field	Value
Operation Code	0xXX
LBA	0xXXXXXX
Transfer Length	0xXX
Control	0xXX

Infusion General Settings

□ Count Randomly

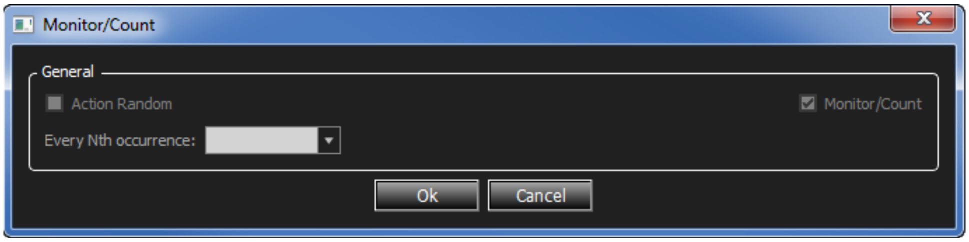
Counter Value: 1

Direction: From P1/P3

Figure 4.34: Adding an Event for Sequence 1

2. Click **OK** to close the 6-Byte Any SCSI Command dialog box.
3. After adding an Event, to add an Action in the Sequence 1 panel, drag and drop Monitor/Count.

   The Monitor/Count dialog box displays.



Monitor/Count

General

□ Action Random

☑ Monitor/Count

Every Nth occurrence:

Figure 4.35: Adding Action Monitor/Count for Sequence 1

4. Click the **OK** button to close the Monitor/Count dialog box.
5. Repeat step 4 to add another Action (if desired).

   The completed Scenario is shown below.

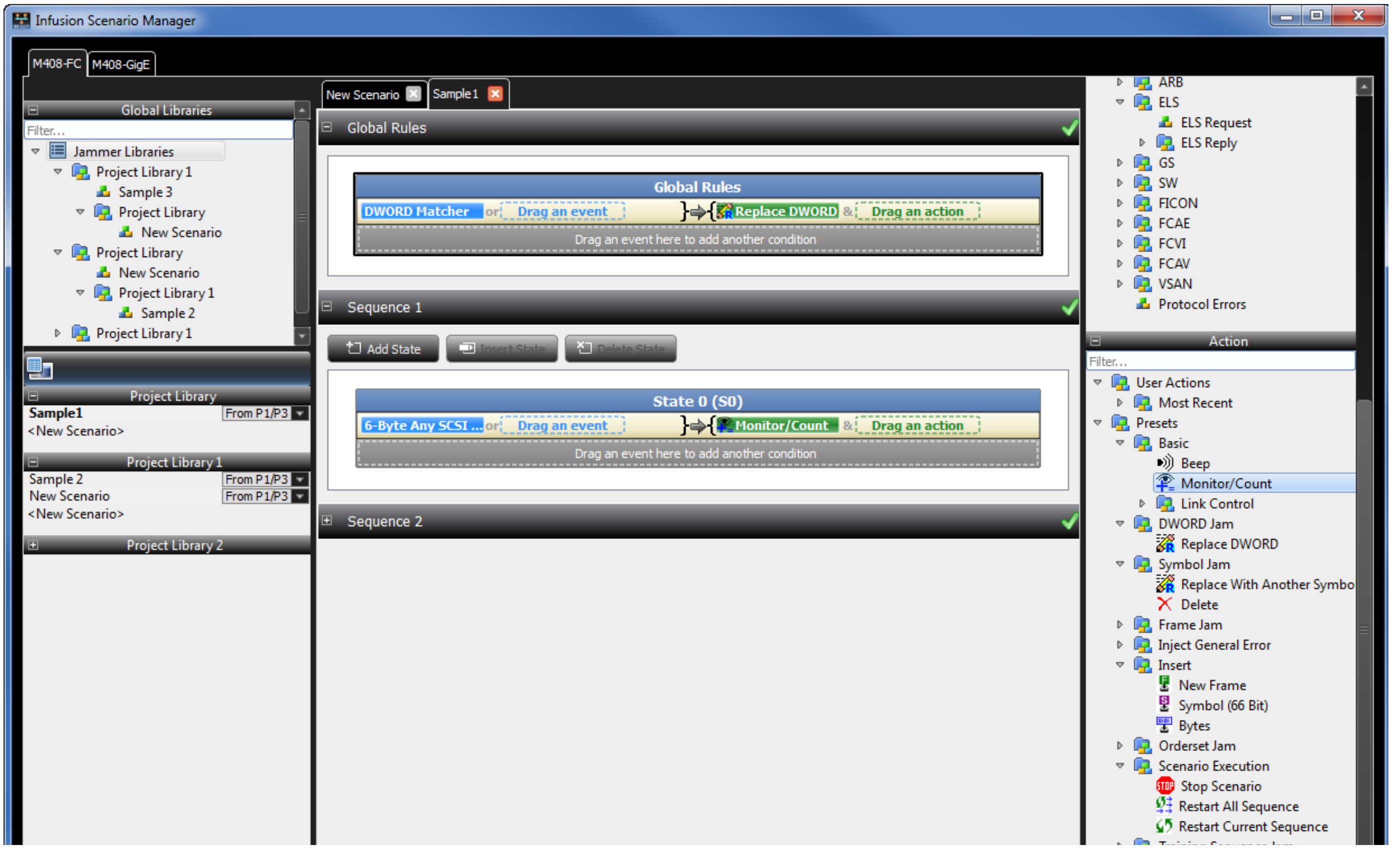


Figure 4.36: Complete Scenario of Insert DWORD Matcher

4.7.2 Sequence Creation

A sequence can have multiple states, but only one state is active at any time. In other words, at any point in time, a sequence “waits” for one Event (or Combined Event) and responds with the corresponding Action or set of Actions when the Event occurs.

A sequence is more powerful than Global Rules, because you can create branching or looping test logic with a sequence.You can include up to two sequences in a Scenario, but each is completely independent of the other. There is no branching or other interaction between the two, except through the Restart All Sequences Action.

You must follow some simple rules when creating sequences:

TABLE 4.6: Sequence Rules

You can use only two branch Actions per state. When you specify Actions for a state, you can only use two instances of **Branch to an Existing State** or **Branch to a New State**. If you try to use more than two, a red error message appears in the status area of the application that says “Too Many Actions.”
You can use only one restart sequence Action per state. When you specify Actions for a state, you can only use one instance of **Restart Current Sequence** or **Restart All Sequences**. If you try to use more than one, a red error message appears in the status area of the application that says “Too Many Actions.”
You can use a maximum of 255 states per sequence. If you try to use more than 255 states, a red error message appears in the status area of the application.

4.7.3 Summary of Scenario Creation

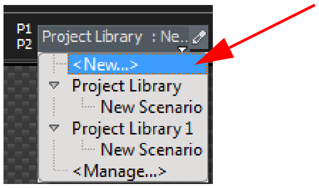
The suggested process of creating and executing a Scenario is as follows:

1. Create a Scenario in the library.
2. Drag and drop to create Global Rules Events and Actions and/or to create Sequence and State Events and Actions.
3. Complete the Scenario and Save it.
4. Select the Scenario in the Library that you want to run on the device.
5. To run the Scenario, click the **Start Session** button. The device starts to monitor/ modify traffic.

4.8 Running Scenarios

If you use a library as a Scenario archive, then the process of executing a Scenario is as follows:

Click on **File > Open** to open an existing File Library. The File Library displays all saved Scenarios in that library and you can select a Scenario.



OR

Select a saved Scenario from the drop-down list and click the **Start Session** button.

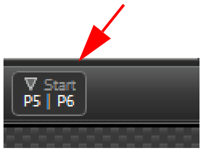
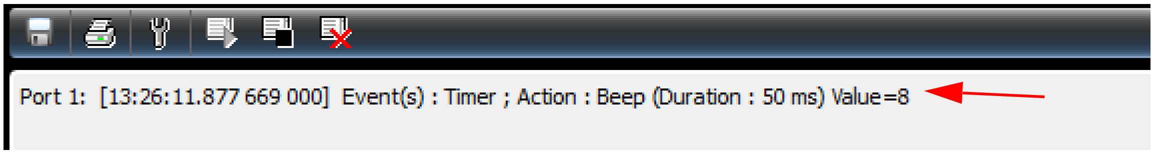


Figure 4.37: Running a Scenario

Once the Scenario is complete or stopped the Output panel displays the Port, Time, Event, Action duration and value.



Port 1: [13:26:11.877 669 000] Event(s) : Timer ; Action : Beep (Duration : 50 ms) Value=8

Figure 4.38: Output Panel Displaying Session Started and Stopped

Chapter 5

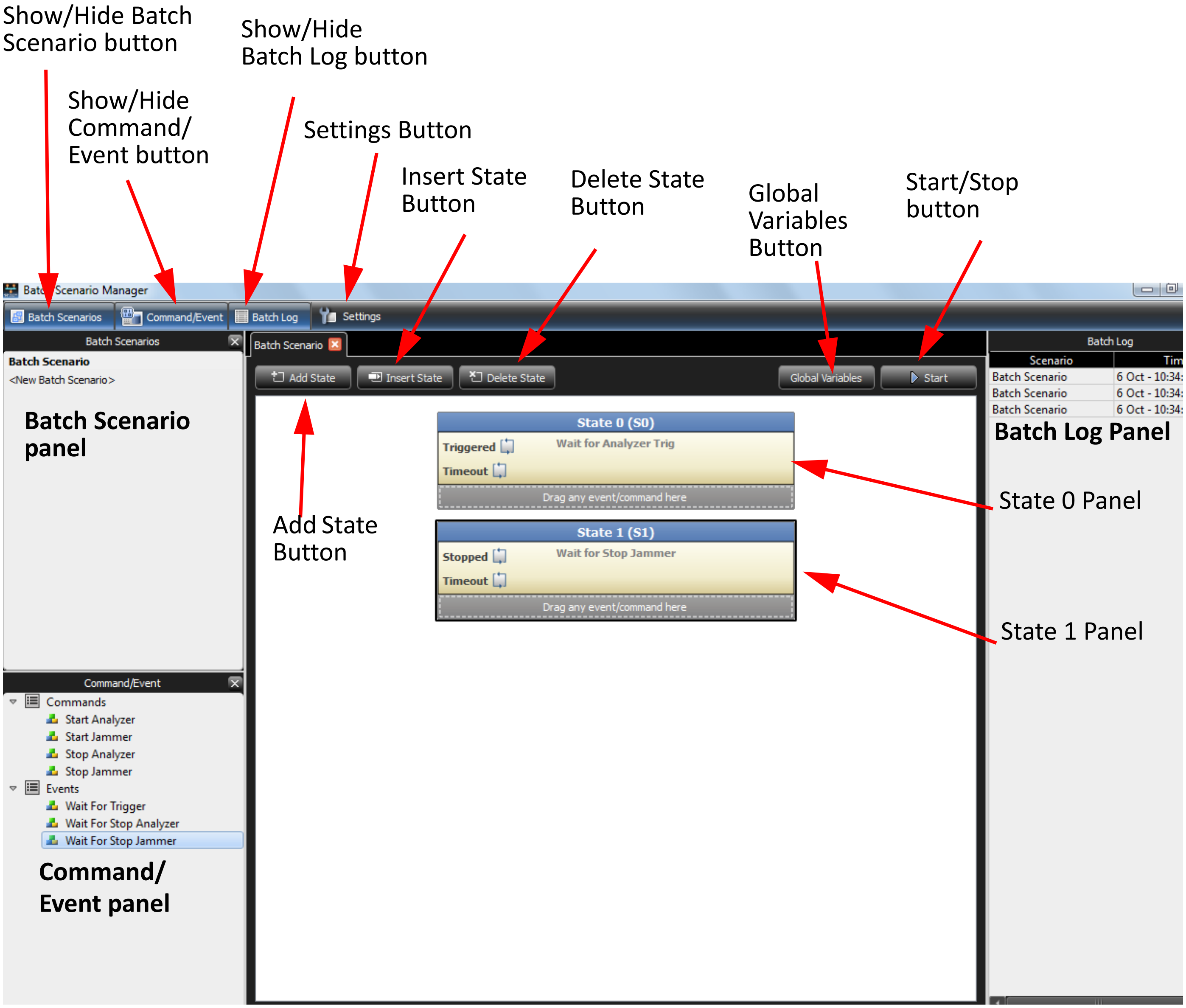
Batch Scenario

5.1 Using the Batch Scenario Feature

You can run a sequence of executable scenarios to control both the Analyzer and the Jammer automatically. A Scenario Batch file is a a list of commands to run in sequence when you execute the file. A batch scenario can manage Jammer scenarios and Analyzer recordings and their assigned ports and hardware in sequence. The system checks for accuracy of inputs and commands.

Once a new Project is defined (see “Starting a New Project” on page 34) you can use the Batch Scenario feature by selecting **File>Batch** to display the Batch Scenario Manager dialog (see Figure 5.1 on page 218). Batch Scenarios are part of a Project, and are saved as such. Each Project file can have a unique set of different Batch Scenarios.

A batch scenario can be repeated up to 10,000 times. Branching to previous states is not permitted, in order to prevent infinite loops.



Scenario	Tim
Batch Scenario	6 Oct - 10:34:
Batch Scenario	6 Oct - 10:34:
Batch Scenario	6 Oct - 10:34:

Figure 5.1: Batch Scenario Manager Dialog.

5.1.1 Interface

The following buttons and panels are available to use the Batch Scenario functions:

- ❑ **Show/Hide Batch Scenario Button:** Toggles between showing/hiding the Batch Scenario pane.
- ❑ **Show/Hide Command/Event Button:** Toggles between showing/hiding the Command/ Event pane.
- ❑ **Show/Hide Batch Log Button:** Toggles between showing/hiding the Batch Log pane.
- ❑ **Add State Button:** Click to add a new state.
- ❑ **Insert State Button:** Click to insert a state after the selected state.
- ❑ **Delete State Button:** Click to delete the selected state.
- ❑ **Start Button:** Click to start the scenario.
- ❑ **Batch Scenario Panel:** Lists all the available Batch Scenarios. Double-click on <**New Batch Scenario**> to create a new scenario. The following operations are available through a right-click context menu:
    - Remove Scenario
    - Rename Scenario
    - Copy Scenario
    - Paste Scenario
- ❑ **Command/Event Panel:** Lists all the available Commands and Events.
- ❑ **Batch Log Panel:** Displays the scenario name, date and time run and description of the scenario.

Note: The log viewer reads up to 1000 entries, but when you save a batch log, it will contain the last 500,000 internal entries.

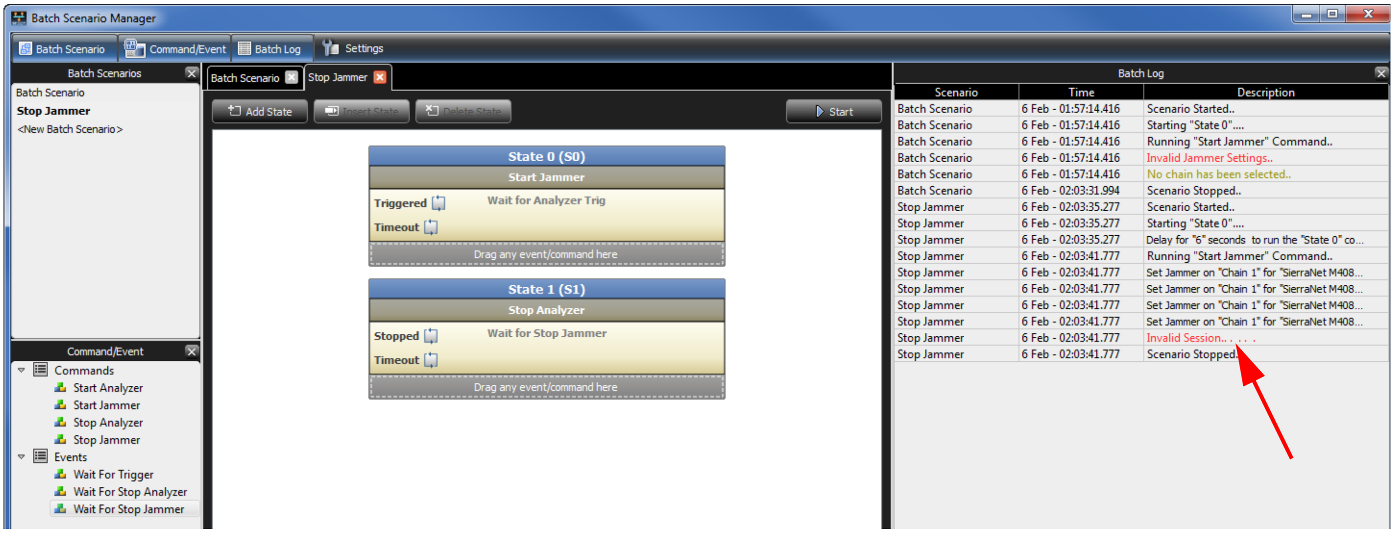
Note: In order to save the jammer log from batch mode, enable "Automatic log" in the Jammer log settings.

5.2 Batch Scenario Overview

You create Batch Scenarios on a host machine running the Net Protocol Suite application. You then specify the Batch Scenarios for execution on a SierraNet platform.

The Net protocol Suite application provides a user friendly interface for building Batch Scenarios. The interface prompts you for simple decisions and choices using buttons and has a drag and drop interface. As you make your selections, the script takes shape automatically in the Batch Scenario window.

Click the **Add State** button, then drag and drop Commands and Events in the new State panels that get created. If invalid actions are assigned, then a red Invalid Session message displays in the Batch Log panel.



Batch Log

Scenario	Time	Description
Batch Scenario	6 Feb - 01:57:14.416	Scenario Started..
Batch Scenario	6 Feb - 01:57:14.416	Starting "State 0"....
Batch Scenario	6 Feb - 01:57:14.416	Running "Start Jammer" Command..
Batch Scenario	6 Feb - 01:57:14.416	Invalid Jammer Settings..
Batch Scenario	6 Feb - 01:57:14.416	No chain has been selected..
Batch Scenario	6 Feb - 02:03:31.994	Scenario Stopped..
Stop Jammer	6 Feb - 02:03:35.277	Scenario Started..
Stop Jammer	6 Feb - 02:03:35.277	Starting "State 0"....
Stop Jammer	6 Feb - 02:03:35.277	Delay for "6" seconds to run the "State 0" co...
Stop Jammer	6 Feb - 02:03:41.777	Running "Start Jammer" Command..
Stop Jammer	6 Feb - 02:03:41.777	Set Jammer on "Chain 1" for "SierraNet M408...
Stop Jammer	6 Feb - 02:03:41.777	Set Jammer on "Chain 1" for "SierraNet M408...
Stop Jammer	6 Feb - 02:03:41.777	Set Jammer on "Chain 1" for "SierraNet M408...
Stop Jammer	6 Feb - 02:03:41.777	Set Jammer on "Chain 1" for "SierraNet M408...
Stop Jammer	6 Feb - 02:03:41.777	Invalid Session.. . . . .
Stop Jammer	6 Feb - 02:03:41.777	Scenario Stopped..

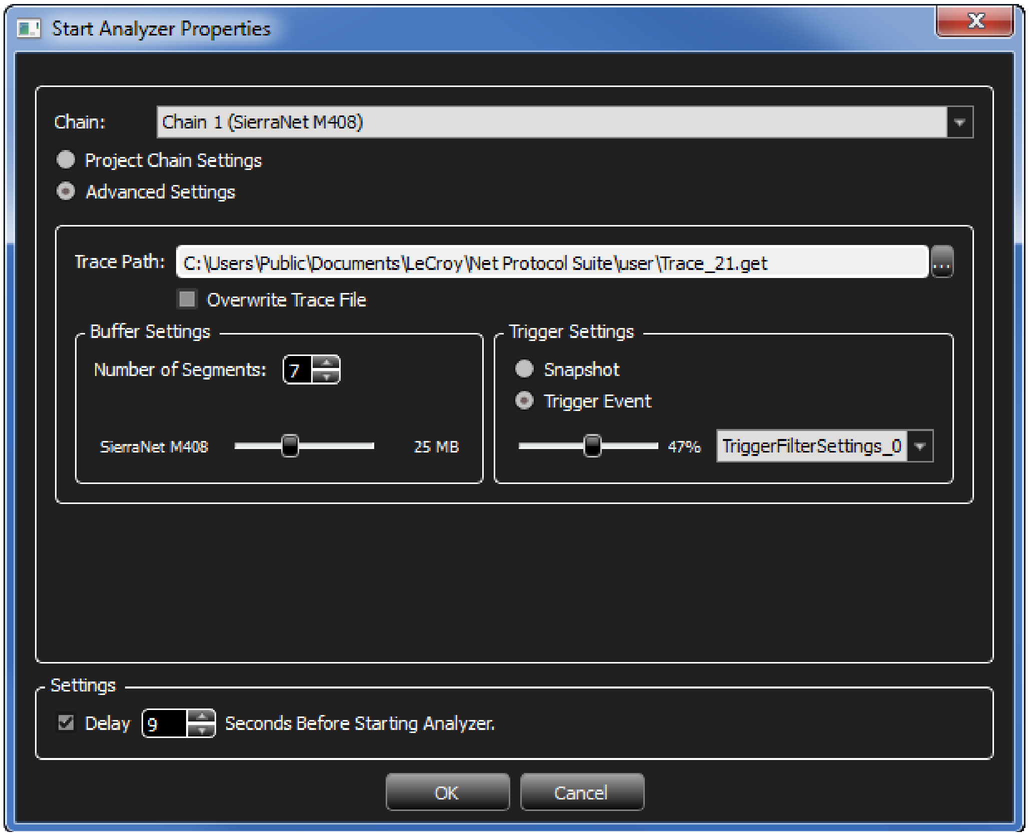
Figure 5.2: Add State Batch Scenario Manager.

5.2.1 Adding Commands

Four types of commands are available:

Start Analyzer

Drag and drop the Start Analyzer command to display the Command Property dialog.



Chain: Chain 1 (SierraNet M408)

○ Project Chain Settings

● Advanced Settings

Trace Path: C:\Users\Public\Documents\LeCroy\Net Protocol Suite\user\Trace_21.get

□ Overwrite Trace File

Buffer Settings

Number of Segments: 7

SierraNet M408 25 MB

Trigger Settings

○ Snapshot

● Trigger Event

47% TriggerFilterSettings_0

Settings

☑ Delay 9 Seconds Before Starting Analyzer.

Figure 5.3: Start Analyzer Command Property Dialog.

Chain: Select a Chain from the drop-down list.

Project Chain Settings: Click this button to select Project Chain Settings.

Advanced Settings: Click this button to select Project Chain Settings to activate the settings below:

Trace Path: Click the ellipsis button to display the Select Trace File Name dialog to save the trace file.

Overwrite Trace File: Select the checkbox to overwrite the trace file.

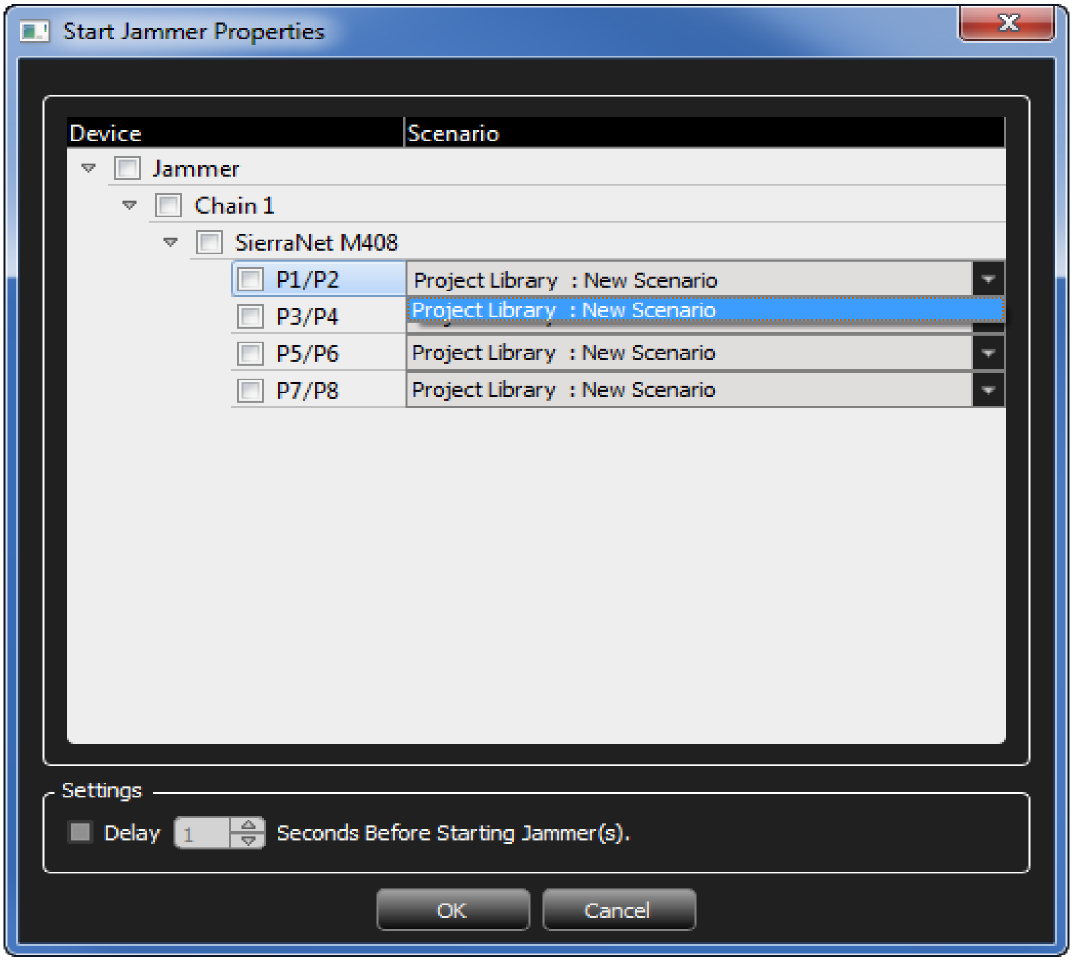
Buffer Settings: Set the number of segments and the buffer size.

Trigger Settings: Select Snapshot or Trigger Event. Select the Trigger Filter Settings from the dropdown list and move the slider to the desired percentage.

If a delay is needed after the command is executed, check the Delay checkbox and set the time in seconds.

Start Jammer

Drag and drop the Start Jammer command to display the Start Jammer Properties dialog.



Device	Scenario
□ Jammer	
□ Chain 1	
□ SierraNet M408	
□ P1/P2	Project Library : New Scenario
□ P3/P4	Project Library : New Scenario
□ P5/P6	Project Library : New Scenario
□ P7/P8	Project Library : New Scenario

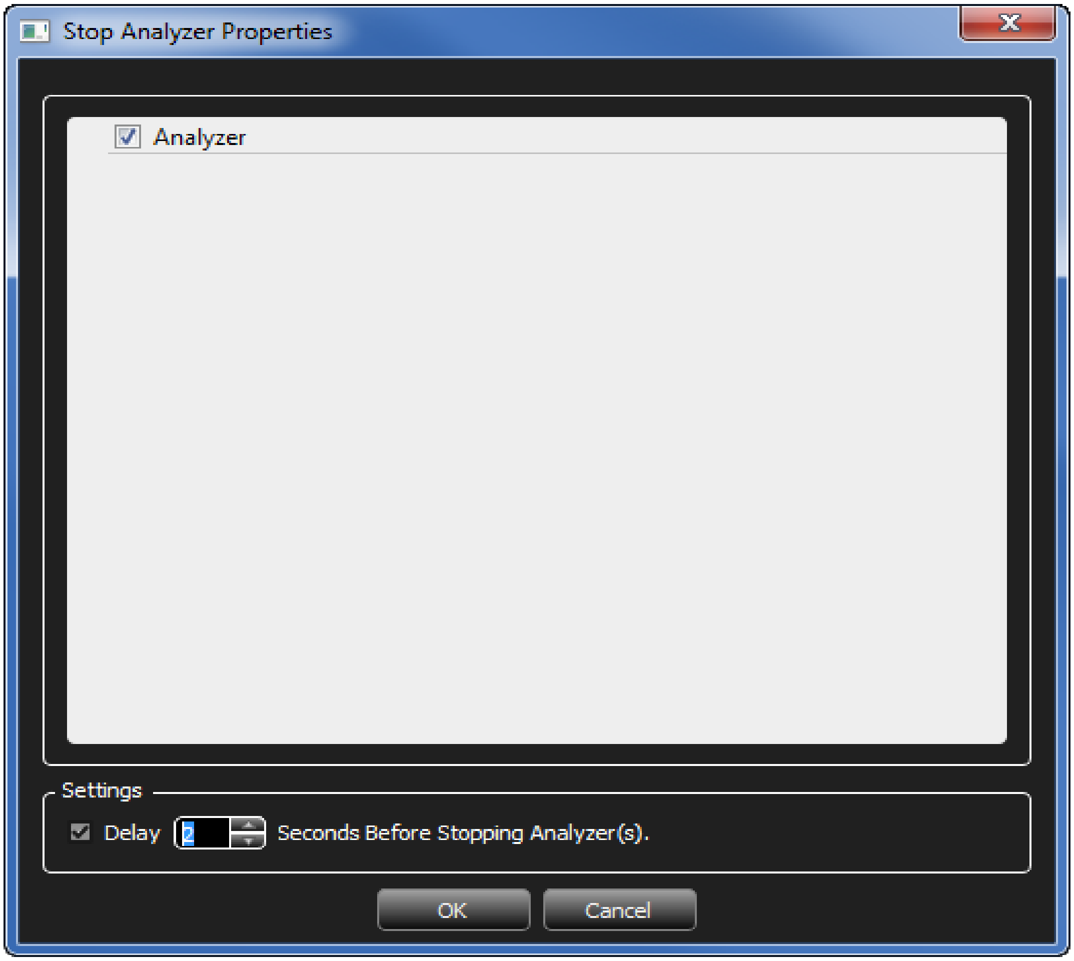
□ Delay 1 Seconds Before Starting Jammer(s).

Figure 5.4: Start Jammer Properties Dialog.

Select the Jammer checkbox to select all four port pairs or select individual port pairs. If a delay is needed after the command is executed, check the Delay checkbox and set the time in seconds.

Stop Analyzer

Drag and drop the Stop Analyzer command to display the Stop Analyzer Properties dialog.



Stop Analyzer Properties

☑ Analyzer

Settings

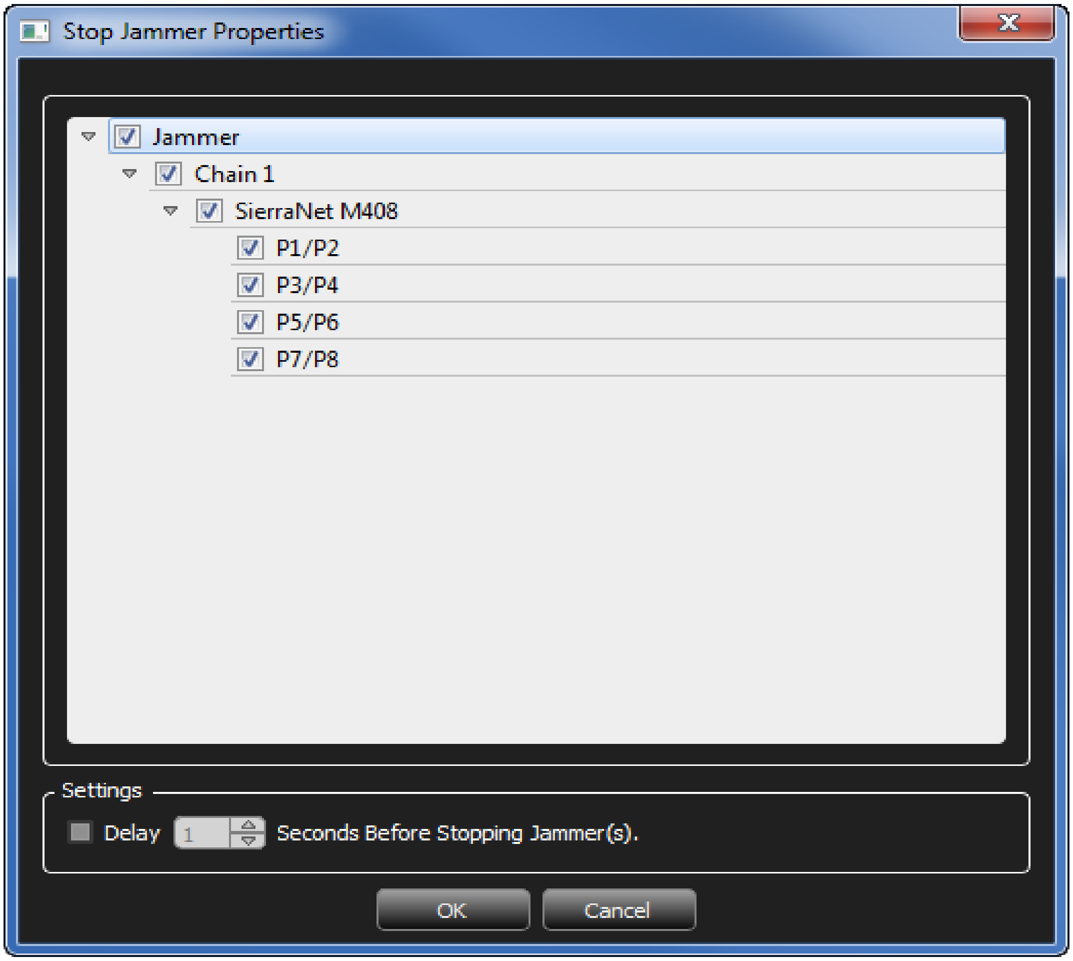
☑ Delay 2 Seconds Before Stopping Analyzer(s).

Figure 5.5: Stop Analyzer Properties Dialog.

Select the Analyzer checkbox. If a delay is needed after the command is executed, check the Delay checkbox and set the time in seconds.

Stop Jammer

Drag and drop the Stop Jammer command to display the Stop Jammer Properties dialog.



Stop Jammer Properties

- ☑ Jammer
  - ☑ Chain 1
    - ☑ SierraNet M408
      - ☑ P1/P2
      - ☑ P3/P4
      - ☑ P5/P6
      - ☑ P7/P8

Settings

□ Delay 1 Seconds Before Stopping Jammer(s).

Figure 5.6: Stop Jammer Properties Dialog.

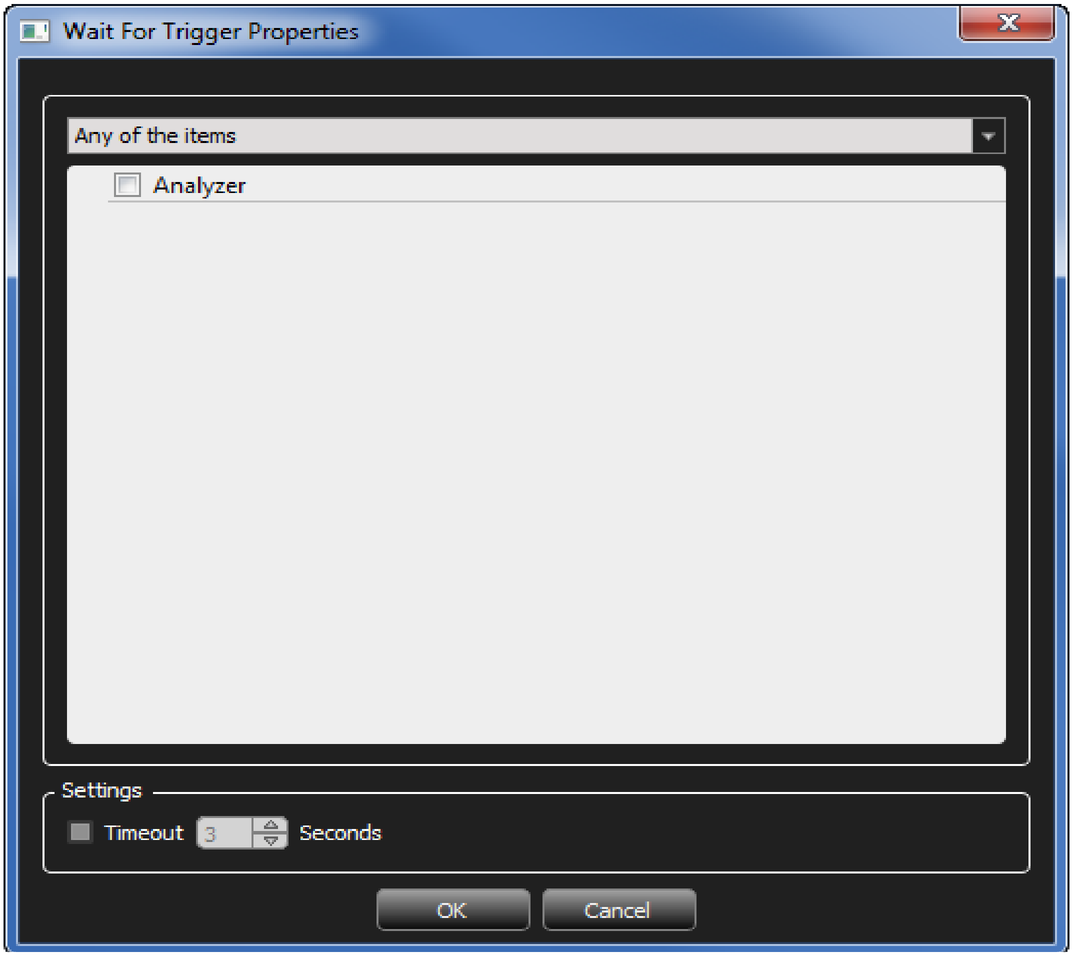
Select the Jammer checkbox to select all four port pairs or select individual port pairs. If a delay is needed after the command is executed, check the Delay checkbox and set the time in seconds.

5.2.2 Adding Events

Three types of events are available:

Wait For Trigger

Drag and drop the Wait For Trigger event to display the Wait For Trigger Properties dialog.



Wait For Trigger Properties

Any of the items

□ Analyzer

Settings

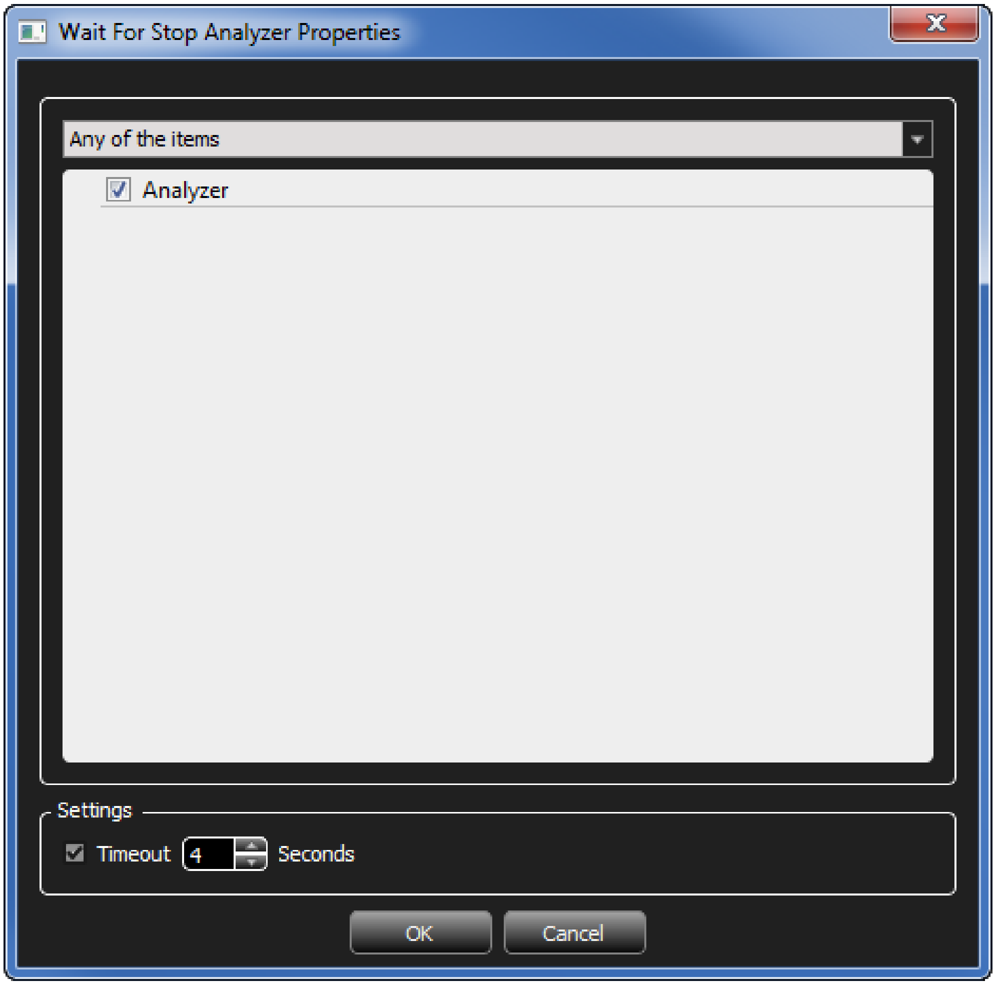
□ Timeout 3 Seconds

Figure 5.7: Wait For Trigger Properties Dialog.

Select an option from the drop-down list. In order to prevent an infinite Wait, you can select the Timeout checkbox and set the time in seconds.

Wait For Stop Analyzer

Drag and drop the Wait For Stop Analyzer event to display the Wait For Stop Analyzer Properties dialog.



Wait For Stop Analyzer Properties

Any of the items

☑ Analyzer

Settings

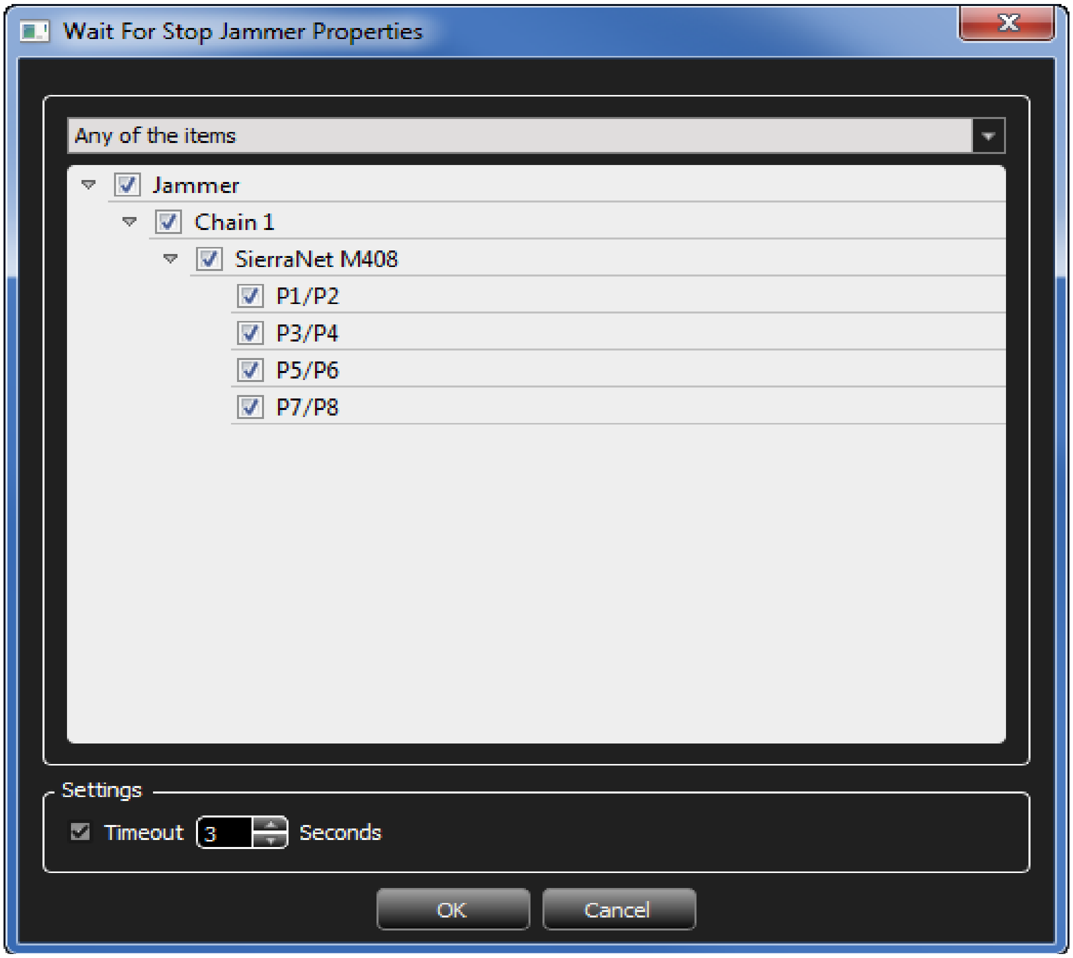
☑ Timeout 4 Seconds

Figure 5.8: Wait For Stop Analyzer Properties Dialog.

Select an option from the drop-down list. In order to prevent an infinite Wait, you can select the Timeout checkbox and set the time in seconds.

Wait For Stop Jammer

Drag and drop the Wait For Stop Jammer event to display the Wait For Stop Jammer Properties dialog.



Any of the items

☑ Jammer
- ☑ Chain 1
  - ☑ SierraNet M408
    - ☑ P1/P2
    - ☑ P3/P4
    - ☑ P5/P6
    - ☑ P7/P8

Settings

☑ Timeout 3 Seconds

Figure 5.9: Wait For Stop Jammer Properties Dialog.

Select the Jammer checkbox to select all four port pairs or select individual port pairs. In order to prevent an infinite Wait, you can select the Timeout checkbox and set the time in seconds.

5.2.3 State Transition

Click on the State Transition icon to change the state to transition to. Left-click for menu options to display as shown in the following screen capture and select the state to transition to. To remove the state transition select **No Jump.**

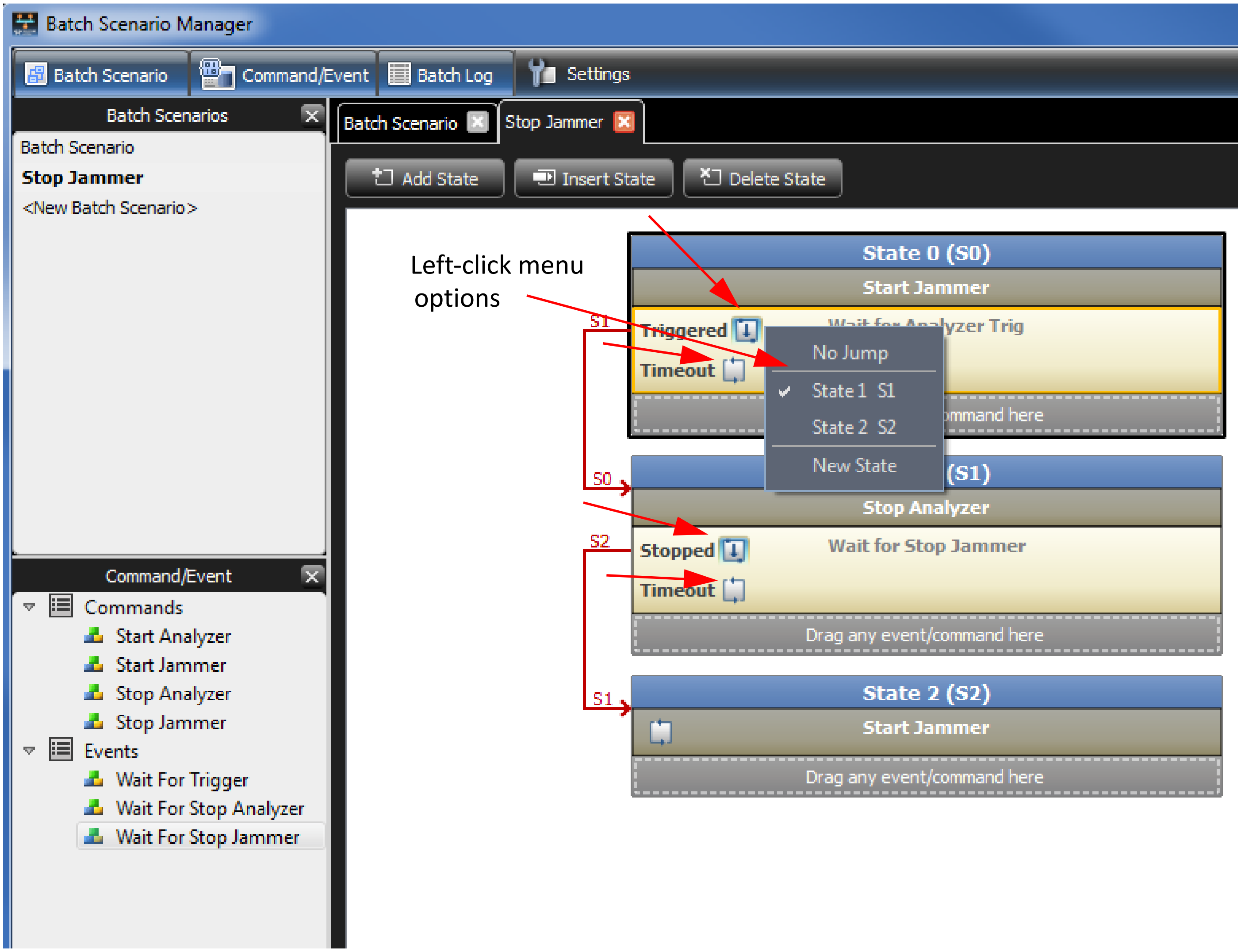


Figure 5.10: State Transition.

5.2.4 Global Variables

Each batch scenario contains a list of global variables which allows you to set data for specific fields of frame events, or trigger setting patterns without editing them one by one. Global variables are automatically applied to all the trigger setting patterns that are selected in the “Start Analyzer” command immediately before you run the command. If you select “Use Project Chain Settings” with the “Start Analyzer” command, global variables will be applied to the current trigger settings.

This also works for the Jammer. Global variables are applied automatically to all frame events of a Jammer scenario that are selected in the “Start Jammer” command, immediately before you run the command.

Global variables have no effect on any trigger settings or Jammer scenarios that are not used in the batch scenario.

Global variables provide dynamically changing event fields in runtime. You can add as many fields as you need to the global variable list and specify your desired value for them. When running batch mode, the software replaces your value in the specified field for any event in which that field is used. The software looks in all events for that field and replaces the value.

Global Variables Dialog

1. To change the definition of selected global variables, go to Batch Scenario Manager and click on the “Global Variables” button.
   - ❑ The Global Variables dialog window opens.

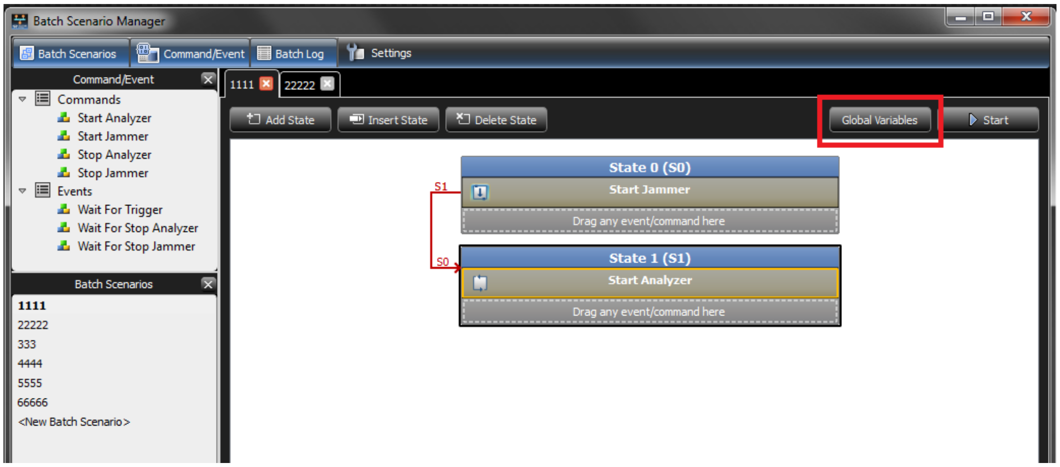
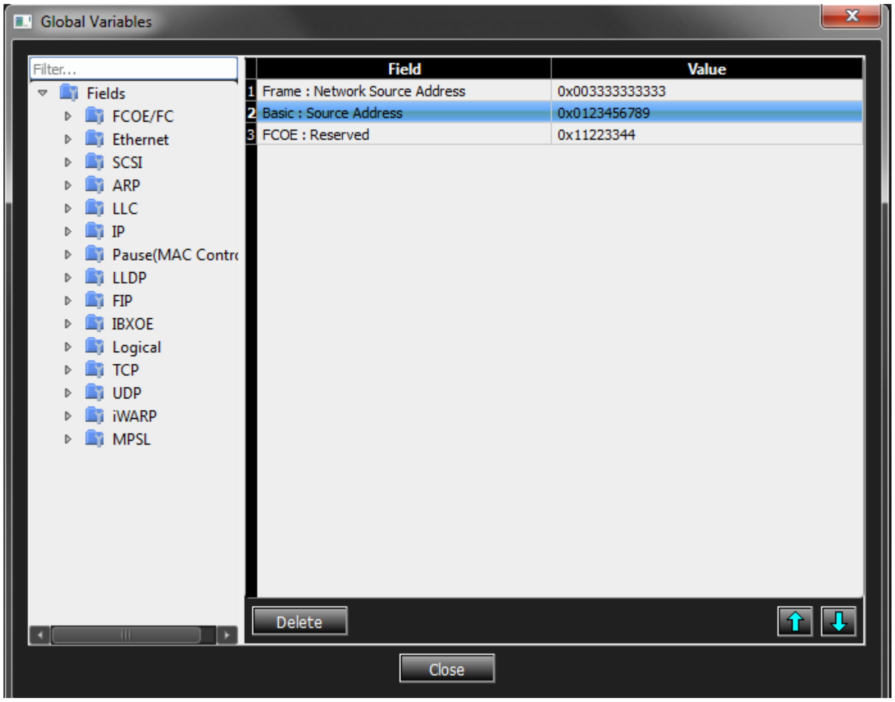


Figure 5.11: Batch Scenario Manager window.



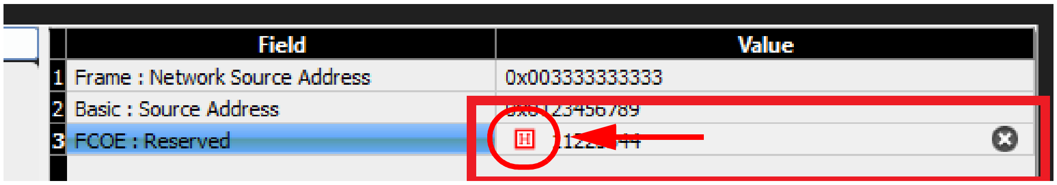
	Field	Value
1	Frame : Network Source Address	0x003333333333
2	Basic : Source Address	0x0123456789
3	FCOE : Reserved	0x11223344

Figure 5.12: Global Variables dialog window.

This window consists of two panes: on the left, a tree of all available fields. On the right is a table of fields that can be selected.

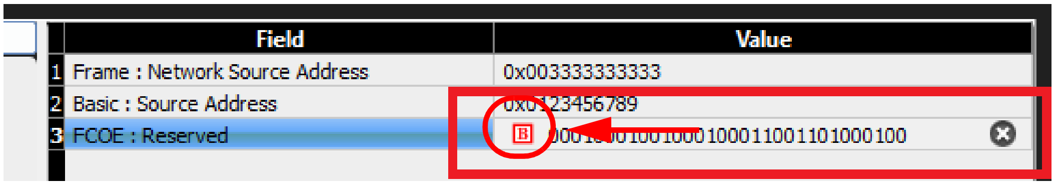
You can add a global variable to the table simply by dragging a field from the tree on the left and dropping it into the table on the right. This adds the field to the table with an empty value. To edit the value, simply double-click on the value cell.

A red "H" appears at the left of the value cell. (See Figure 5.13.) This shows, by default, that the value is to be in hexadecimal format. You can switch between binary and hexadecimal by simply clicking on the red H; it changes to a red "B" for binary. (See Figure 5.14.)



	Field	Value
1	Frame : Network Source Address	0x003333333333
2	Basic : Source Address	0x0123456789
3	FCOE : Reserved	H 0x11223344

Figure 5.13: Hexadecimal button.



	Field	Value
1	Frame : Network Source Address	0x003333333333
2	Basic : Source Address	0x0123456789
3	FCOE : Reserved	B 00010001001000100011001101000100

Figure 5.14: Binary button.

There is no length limit for the value, but it may trimmed according to field length when it is applied to a frame pattern or event.

To remove a global variable, simply select it on the table and select the Delete button. The variable is removed from the right pane of the dialog.

The Up and Down arrows (Figure 5.15) let you rearrange the order of variable values that you wish to change, before Net Protocol Suite runs a scenario. For most fields, the order does not matter, but for the fields that do change the format of events, this order becomes important. For example, suppose you want to change the value of the field **Opcode** in a SCSI command, and then change one of the other fields in that SCSI command. You will have to move the Opcode field to the top of the list, because when you set Opcode fields, the event fields will be changed automatically. Then you can change the value of another field. On the other hand, if you want to set the value of a field such as **Originator S_ID**, changing its value has no effect on the format of other fields in an event, so you don't need to specify the order in which these fields are accessed.

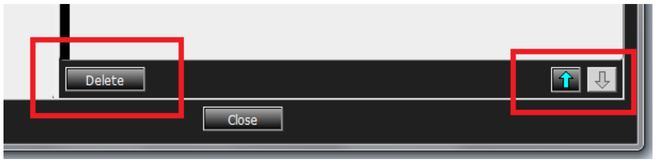


Figure 5.15: Location of Delete button and Up and Down arrows.

Note: Replacing any value in a frame pattern or event may cause other fields values to reset. To avoid this, make sure you select the correct order of global variables.

For example, assume there is a batch scenario with one "Start Jammer" command and global variables as shown in Figure 5.16 and Figure 5.17.

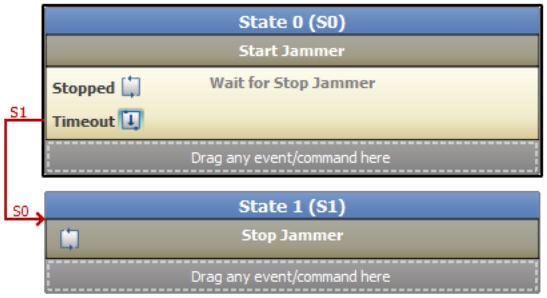
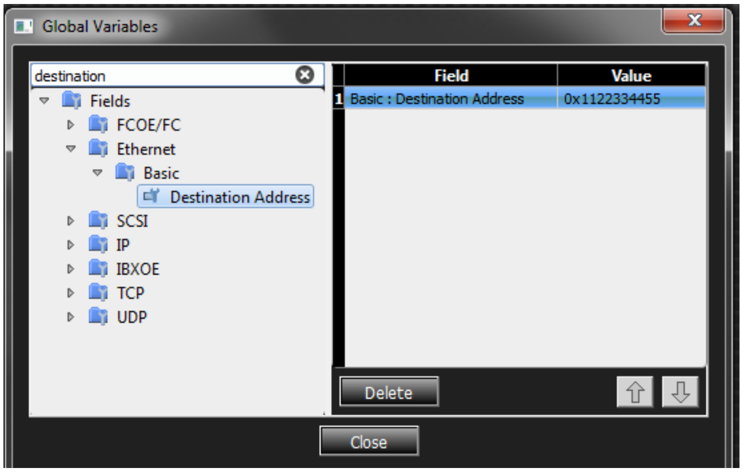


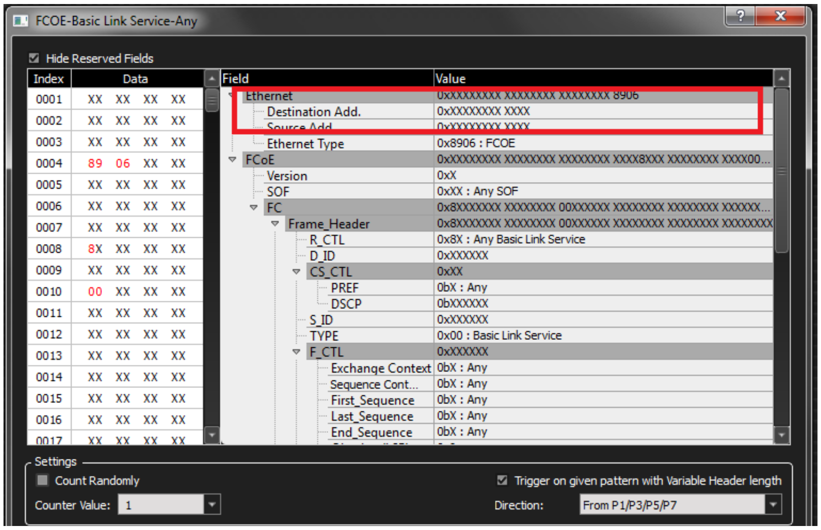
Figure 5.16: Example of a Batch Scenario.



	Field	Value
1	Basic : Destination Address	0x1122334455

Figure 5.17: Destination Address field selected.

A batch scenario such as this can run a jammer scenario with a frame event. An example is shown in Figure 5.18.



☑ Hide Reserved Fields

Index	Data			
0001	XX	XX	XX	XX
0002	XX	XX	XX	XX
0003	XX	XX	XX	XX
0004	89	06	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	8X	XX	XX	XX
0009	XX	XX	XX	XX
0010	00	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX
0015	XX	XX	XX	XX
0016	XX	XX	XX	XX
0017	XX	XX	XX	XX

Field	Value
Ethernet	0xXXXXXXXX XXXXXXXX XXXXXXXX 8906
Destination Add.	0xXXXXXXXX XXXX
Source Add.	0xXXXXXXXX XXXX
Ethernet Type	0x8906 : FCOE
FCoE	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXX8XXX XXXXXXXX XXXX00...
Version	0xX
SOF	0xXX : Any SOF
FC	0x8XXXXXXX XXXXXXXX 00XXXXXX XXXXXXXX XXXXXXXX XXXXXX...
Frame_Header	0x8XXXXXXX XXXXXXXX 00XXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
R_CTL	0x8X : Any Basic Link Service
D_ID	0xXXXXXX
CS_CTL	0xXX
PREF	0bX : Any
DSCP	0bXXXXXX
S_ID	0xXXXXXX
TYPE	0x00 : Basic Link Service
F_CTL	0xXXXXXX
Exchange Context	0bX : Any
Sequence Cont...	0bX : Any
First_Sequence	0bX : Any
Last_Sequence	0bX : Any
End_Sequence	0bX : Any

Settings

□ Count Randomly

Counter Value: 1

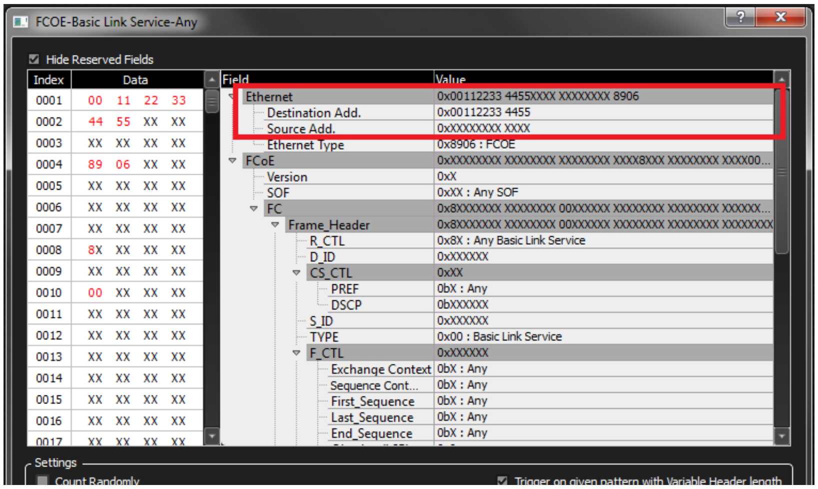
☑ Trigger on given pattern with Variable Header length

Direction: From P1/P3/P5/P7

Figure 5.18: Destination Address before changes.

As you see, the “Destination Address” field is 0xXXXXXXXX XXXX. After starting the batch scenario, the expected behavior is the “Destination Address” field is replaced with the value 0x1122334455 from the defined global variable.

If you check the same jammer frame event after running the batch, the result will be as seen in Figure 5.19, which is the expected behavior.



FCOE-Basic Link Service-Any

☑ Hide Reserved Fields

Index	Data			
0001	00	11	22	33
0002	44	55	XX	XX
0003	XX	XX	XX	XX
0004	89	06	XX	XX
0005	XX	XX	XX	XX
0006	XX	XX	XX	XX
0007	XX	XX	XX	XX
0008	8X	XX	XX	XX
0009	XX	XX	XX	XX
0010	00	XX	XX	XX
0011	XX	XX	XX	XX
0012	XX	XX	XX	XX
0013	XX	XX	XX	XX
0014	XX	XX	XX	XX
0015	XX	XX	XX	XX
0016	XX	XX	XX	XX
0017	XX	XX	XX	XX

Field	Value
Ethernet	0x00112233 4455XXXX XXXXXXXX 8906
Destination Add.	0x00112233 4455
Source Add.	0xXXXXXXXX XXXX
Ethernet Type	0x8906 : FCOE
FCoE	0xXXXXXXXX XXXXXXXX XXXXXXXX XXXX8XXX XXXXXXXX XXXX00...
Version	0xX
SOF	0xXX : Any SOF
FC	0x8XXXXXXX XXXXXXXX 00XXXXXX XXXXXXXX XXXXXXXX XXXXXX...
Frame_Header	0x8XXXXXXX XXXXXXXX 00XXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
R_CTL	0x8X : Any Basic Link Service
D_ID	0xXXXXXX
CS_CTL	0xXX
PREF	0bX : Any
DSCP	0bXXXXXX
S_ID	0xXXXXXX
TYPE	0x00 : Basic Link Service
F_CTL	0xXXXXXX
Exchange Context	0bX : Any
Sequence Cont...	0bX : Any
First_Sequence	0bX : Any
Last_Sequence	0bX : Any
End_Sequence	0bX : Any

Settings

□ Count Randomly

☑ Trigger on given pattern with Variable Header length

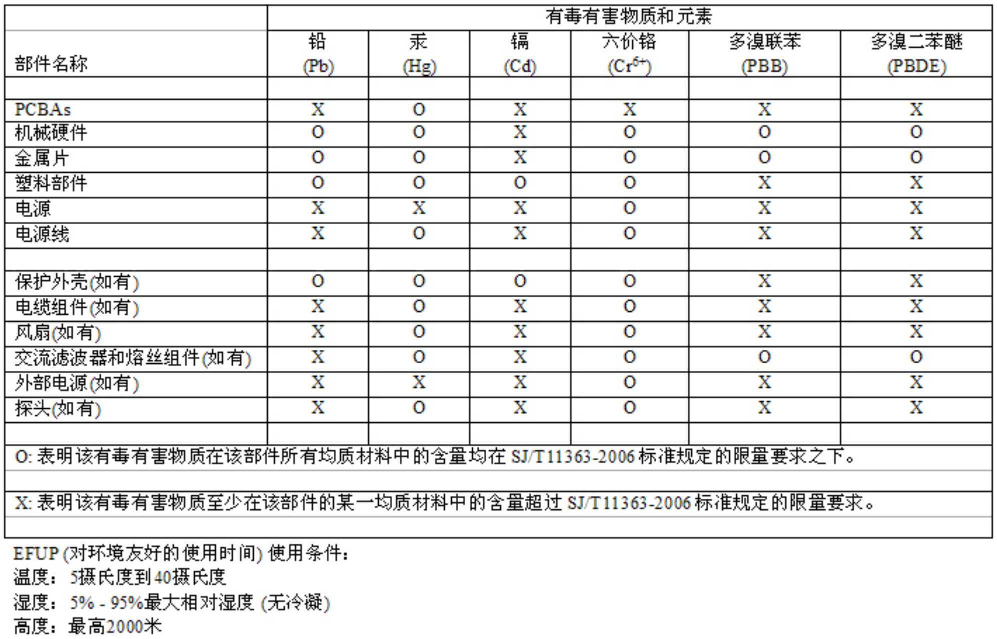
Figure 5.19: Destination Address after changes.

Note: This function makes changes in the actual frame pattern/event which will result in changes in your project.

Appendix A

China Restriction of Hazardous Substances Table

The following tables are supplied in compliance with China's Restriction of Hazardous Substances (China RoHS) requirements:

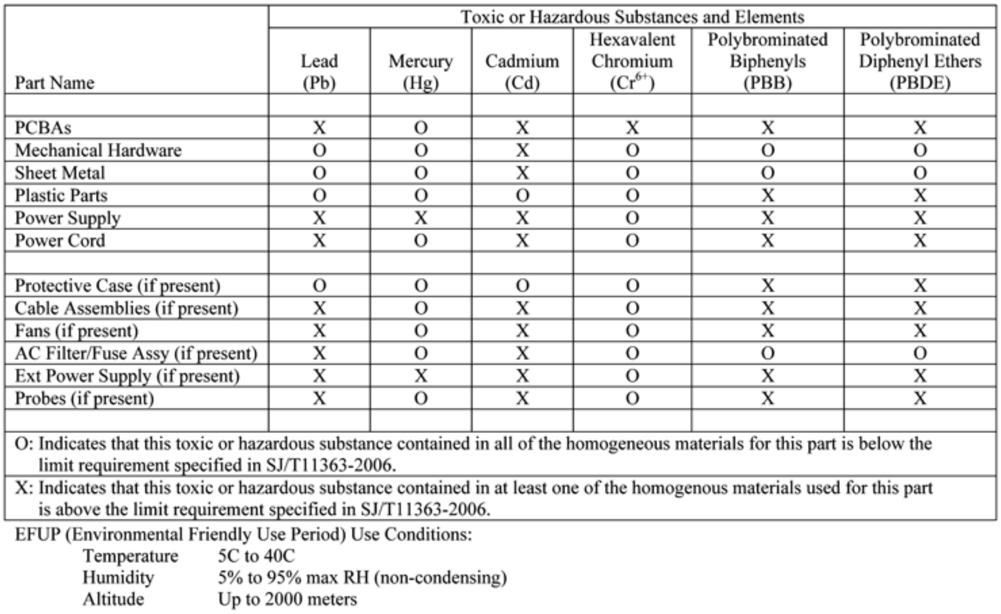


	有毒有害物质和元素					
部件名称	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
PCBAs	X	O	X	X	X	X
机械硬件	O	O	X	O	O	O
金属片	O	O	X	O	O	O
塑料部件	O	O	O	O	X	X
电源	X	X	X	O	X	X
电源线	X	O	X	O	X	X
保护外壳(如有)	O	O	O	O	X	X
电缆组件(如有)	X	O	X	O	X	X
风扇(如有)	X	O	X	O	X	X
交流滤波器和熔丝组件(如有)	X	O	X	O	O	O
外部电源(如有)	X	X	X	O	X	X
探头(如有)	X	O	X	O	X	X

O: 表明该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T11363-2006 标准规定的限量要求之下。

X: 表明该有毒有害物质至少在该部件的某一均质材料中的含量超过 SJ/T11363-2006 标准规定的限量要求。

EFUP (对环境友好的使用时间) 使用条件：
温度： 5摄氏度到40摄氏度
湿度： 5% - 95%最大相对湿度 (无冷凝)
高度： 最高2000米



	Toxic or Hazardous Substances and Elements					
Part Name	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr^{6+})	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCBAs	X	O	X	X	X	X
Mechanical Hardware	O	O	X	O	O	O
Sheet Metal	O	O	X	O	O	O
Plastic Parts	O	O	O	O	X	X
Power Supply	X	X	X	O	X	X
Power Cord	X	O	X	O	X	X
Protective Case (if present)	O	O	O	O	X	X
Cable Assemblies (if present)	X	O	X	O	X	X
Fans (if present)	X	O	X	O	X	X
AC Filter/Fuse Assy (if present)	X	O	X	O	O	O
Ext Power Supply (if present)	X	X	X	O	X	X
Probes (if present)	X	O	X	O	X	X

O: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement specified in SJ/T11363-2006.

X: Indicates that this toxic or hazardous substance contained in at least one of the homogenous materials used for this part is above the limit requirement specified in SJ/T11363-2006.

EFUP (Environmental Friendly Use Period) Use Conditions:

Temperature	5C to 40C
Humidity	5% to 95% max RH (non-condensing)
Altitude	Up to 2000 meters

Appendix B

How to Contact Teledyne LeCroy

Type of Service	Contact	
Call for technical support	US and Canada: Worldwide:	1 (800) 909-7112 1 (408) 653-1260
Fax your questions	Worldwide:	1 (408) 727-6622
Write a letter		Teledyne LeCroy Protocol Solutions Group Customer Support 3385 Scott Blvd. Santa Clara, CA 95054-3115 USA
Send e-mail		psgsupport@teledynelecroy.com
Visit Teledyne LeCroy’s web site		teledynelecroy.com/
Tell Teledyne LeCroy	Report a problem to Teledyne LeCroy Support via e-mail by selecting **Help>Tell Teledyne LeCroy** from the application toolbar. This requires that an e-mail client be installed and configured on the host machine.	

Index